

On biunimodular vectors for unitary matrices

Hartmut Führ, Ziemowit Rzeszutnik

June 23, 2015

Abstract

A biunimodular vector of a unitary matrix $A \in U(n)$ is a vector $v \in \mathbb{T}^n \subset \mathbb{C}^n$ such that $Av \in \mathbb{T}^n$ as well. Over the last 30 years, the sets of biunimodular vectors for Fourier matrices have been the object of extensive research in various areas of mathematics and applied sciences. Here, we broaden this basic harmonic analysis perspective and extend the search for biunimodular vectors to arbitrary unitary matrices. This search can be motivated in various ways. The main motivation is provided by the fact, that the existence of biunimodular vectors for an arbitrary unitary matrix allows for a natural understanding of the structure of all unitary matrices.

Note

As we have learned from the referees, the existence of biunimodular vectors for an arbitrary unitary matrix has been recently proved in this journal by Idel and Wolf (see [36]) basing on the results of [9] in symplectic geometry due to Biran, Entov and Polterovich. In this paper we provide an independent account of this existence phenomenon and push a bit further the theory of biunimodular vectors.

Outline

In Section 1 we describe the background for this research. The next two sections discuss the structure of all unitary matrices via decompositions based on biunimodular vectors. In Section 4 we state the problem of finding biunimodular vectors in several equivalent terms. One of them is a maximal torus decomposition of $SU(n)$, that can be viewed as a close relative of the spectral theorem. In the following sections we justify that all matrices in $U(2)$ and $U(3)$ possess biunimodular vectors and provide two closed formulas for $U(3)$. One of them being an analogue of the standard Euler-Tait-Bryan decomposition of $O(3)$. In Section 8 we provide a simplified novel method to synthesise all matrices in $U(2^n)$, that enjoys an elementary proof for all $n \in \mathbb{N}$. Section 9 is devoted to the study of biunimodular vectors in the general case from the Lie groups perspective. Using basic tools we show that in arbitrary dimension n , the set of matrices possessing biunimodular vectors contains a nonempty open subset of $U(n)$. We also obtain that, up to normalization, the set of biunimodular vectors is finite for almost every unitary matrix. Finally, we employ a simple alternating projection algorithm that for a numerically given unitary matrix produces vectors, that are biunimodular within a set precision. We test this algorithm to provide numerical evidence indicating its effectiveness in finding such near biunimodular vectors for random unitary matrices with dimensions up to 100. We also apply the algorithm to Fourier matrices, and compare the search results to the known solutions.

1 Background

The paper explores the notion of a **biunimodular vector** that traces back to Gauss. The classic example of such vectors are *Gauss sequences* given for $k = 0, 1, \dots, n-1$ as

$$\begin{aligned} u_k &= ce^{\frac{2\pi i}{n}(\lambda k^2 + \mu k)} & n \text{ odd,} \\ u_k &= ce^{\frac{2\pi i}{n}(\frac{\lambda}{2}k^2 + \mu k)} & n \text{ even,} \end{aligned}$$

where $\lambda, \mu \in \{0, 1, \dots, n-1\}$ with λ relatively prime to $n \in \mathbb{N}$ and $c \in \mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$. These vectors are *unimodular*, that is, $|u_k| = 1$ for all $k = 0, 1, \dots, n-1$ and have an interesting property. Their Fourier transform $F_n u$, defined by applying to u the unitary $n \times n$ matrix F_n with entries $(F_n)_{j,k} = \frac{1}{\sqrt{n}} e^{-2\pi i \frac{jk}{n}}$, is unimodular as well.¹

Following Haagerup ([34]) and Saffari ([44]) we attribute the starting point of the general theory of biunimodular vectors to Per Enflo. In 1983 he has asked whether for prime n the only unimodular vectors of length n whose Fourier transform is also unimodular are Gauss sequences. While the answer is affirmative when $n \leq 5$, a computer search done by Björck for $n = 7$ provided a surprising counterexample

$$(1, 1, 1, e^{i\theta}, 1, e^{i\theta}, e^{i\theta}),$$

with $\theta = \arccos(-\frac{3}{4})$ yielding $e^{i\theta} = -\frac{3}{4} + i\frac{\sqrt{7}}{4}$. These findings, published in 1985 ([10]), have been generalized in [11] and later the term “bi-unimodular sequence” has been coined by Björck and Saffari to describe a unimodular finite vector, whose Fourier transform is unimodular as well (see [14]).

The Björck sequences provided in [11] are biunimodular vectors of a prime length p . For $p \equiv -1 \pmod{4}$ their coefficients are either 1 or $e^{i\theta}$ with $\theta = \arccos \frac{1-p}{1+p}$. For $p \equiv 1 \pmod{4}$ their coefficients are either 1, $e^{i\eta}$ or $e^{-i\eta}$ with $\eta = \arccos \frac{1}{\sqrt{p+1}}$. The importance of Björck sequences has been underlined in [6], where it was shown that for these sequences (contrary to Gauss sequences) the discrete narrow band ambiguity function has an optimal bound. However, Gauss and Björck sequences provide only a glimpse at the structure of biunimodular vectors for F_n . Even in the case $p = 7$ there is another such vector found by Björck and Fröberg that is related neither to a Gauss nor to a Björck sequence (see [12] or [34]).

Moreover, in [14] Björck and Saffari proved that if n is divisible by a square, then there are infinitely many (continuum) biunimodular vectors with the leading entry 1, and they conjectured that for all square-free n the number of such biunimodular vectors is finite.

Conjecture 1.1. (Björck, Saffari) *If $n \in \mathbb{N}$ is not divisible by a square, then the set of biunimodular vectors (with the leading entry 1) for the Fourier matrix F_n is finite.*

An easy observation is that a unimodular vector $u = (u_0, u_1, \dots, u_{n-1})$ is biunimodular for F_n if and only if its cyclic translations are orthogonal. This orthogonality relation is called *zero autocorrelation* and means that

$$\sum_{k=0}^{n-1} u_k \overline{u_{k+i}} = 0 \quad \text{for } i = 1, 2, \dots, n-1, \quad (1)$$

where the index $k+i$ is taken $(\text{mod } n)$.

¹ As a matter of fact, the Fourier transform of a Gauss sequence yields another Gauss sequence.

The idea of Björck to search for biunimodular vectors u for F_n relies on setting $x_k = \frac{u_{k+1}}{u_k}$, where $k = 0, 1, \dots, n-1$ with $u_n = u_0$ and transforming (1) to the following set of equations:

$$\begin{aligned} x_0 + x_1 + \dots + x_{n-1} &= 0 \\ x_0x_1 + x_1x_2 + \dots + x_{n-1}x_0 &= 0 \\ &\vdots \\ x_0x_1 \dots x_{n-2} + \dots + x_{n-1}x_0 \dots x_{n-3} &= 0 \\ x_0x_1 \dots x_{n-1} &= 1 \end{aligned} \tag{2}$$

The unimodular solutions of the above set of equations are in one-to-one correspondence to biunimodular vectors for F_n (with the leading entry 1). The general complex solutions of (2) are called *cyclic n -roots* and became a research area of independent interest. In the mid-1980s Arnborg has asked Davenport to establish whether the set of cyclic 6-roots is finite, leading to the popularisation of the cyclic n -roots problem in [22]. Backelin proved in [2] that for n divisible by a square the number of cyclic n -roots is infinite. For $2 \leq n \leq 8$ all cyclic n -roots were found by Björck and Fröberg (see [12, 13, 3]) by using Gröbner basis techniques to solve the system (2). Faugère has found cyclic 9 and 10 roots by improving the search for the Gröbner basis (see [27] and [28]). These results have been confirmed and extended by polyhedral homotopy continuation methods applied for solving (2) as a benchmark problem. The numbers of cyclic n -roots for a square-free n between 2 and 14 is listed below.²

n	2	3	5	6	7	10	11	13	14	15
cyclic n -roots	2	6	70	156	924	34,940	184,756	2,704,156	8,464,307	?
biuni vectors	2	6	20	48	532	?	?	53,222	?	?

The table also contains information about the number of unimodular cyclic n -roots that yields the amount of biunimodular vectors for F_n . The numbers up to $n = 7$ were given by Björck, Fröberg and Haagerup, who inspected the obtained cyclic n -roots to check for unimodular solutions, establishing the real benchmark for solving the cyclic n -root problem (see [12] and [34]). The number of biunimodular vectors for $n = 13$ has been obtained by Gabidulin and Shorin in [30].

Basing on the number of cyclic p -roots for prime p up to 7 Fröberg concluded that the amount of cyclic p -roots should be $\binom{2p-2}{p-1}$. This conjecture has been confirmed by Haagerup in [35] under the condition that the roots are counted with multiplicities.

Theorem 1.2. (Haagerup) *For prime p the number of cyclic p -roots counted with multiplicities is $\binom{2p-2}{p-1}$.*

The paper of Haagerup contains an elegant direct argument showing that the number of cyclic p -roots is finite for prime p , confirming Conjecture 1.1 in the prime case. His more advanced reasoning allows to count the cyclic p -roots with multiplicities, imposing a question whether for all primes cyclic p -roots have multiplicity 1 and providing an additional motivation to verify the number of distinct cyclic 13-roots.

A slightly different approach towards finding biunimodular vectors for F_n has been taken by Gabidulin and Shorin. In [30] they multiplied the system (1) by the product $\prod_{k=0}^{n-1} u_k$ to obtain a system of equations that has been treated with Gröbner basis techniques as well, providing the mentioned number of biunimodular vectors for F_{13} .

The theory of biunimodular vectors may be hard to follow due to their popularity stemming from applications in several fields of signal processing. This popularity can be measured by the amount of various names given to the same objects by many researchers working

²For $2 \leq n \leq 11$ the amount of roots has been verified by various methods, for $n = 13$ and 14 the number of cyclic n -roots is claimed only by Li and Tsai (see [40]). Moreover, they count only isolated roots, so the number of cyclic 14-roots still has to be verified as finite or not.

within the area. Gauss sequences are often called Zadoff, Chu or Wiener sequences. Unimodular vectors are described as constant amplitude, phase-shift keyed or polyphase sequences. Vectors whose Fourier transform is unimodular are named as perfect, having optimum correlation or zero autocorrelation. Therefore, biunimodular vectors are studied as CAZAC (constant amplitude zero autocorrelation) sequences, PSK (phase-shift keyed) perfect sequences, polyphase sequences with optimum correlation and so on (see [7] by Benedetto *et al.* for a better account of this nomenclature and a list of relevant papers that can be extended by adding an early reference [1]).

Since full understanding of biunimodular vectors would allow to resolve the circulant Hadamard matrix conjecture, and is just a tip of the iceberg being a classification of all Hadamard matrices, the complexity of the topic is apparent.

It is important to notice, that the research on biunimodular vectors is not confined to the Fourier transform F_n on the cyclic group \mathbb{Z}_n . Indeed, real biunimodular vectors for the Fourier transform on the group $(\mathbb{Z}_2)^n$ are investigated under the name of *bent functions*. Here n must be even and the number of bent functions is known for $n \leq 8$. The latest count is due to Langevin and Leander who proved the number to be 99270589265934370305785861242880 in the case $n = 8$ (see [39]).

In [31] it has been proved that biunimodular vectors exist for the Fourier transform on any finite abelian group. This raises the question of existence of such vectors for an arbitrary unitary matrix and motivates the following

Definition 1.3. *Let A be an $n \times n$ unitary matrix. A vector $v \in \mathbb{C}^n$ is called a **biunimodular vector** for A if both v and Av are unimodular (i.e. have all entries of modulus one).*

One can argue that the above notion has surfaced already in works on the problem of mutually unbiased bases (MUB). Indeed, the problem can be brought down to finding all biunimodular vectors for a given complex $n \times n$ Hadamard matrix and checking for a subcollection of these vectors that forms an orthonormal basis of \mathbb{C}^n . This approach has been used in [33] by Grassl for F_6 and by Bengtsson *et al.* for some other 6×6 Hadamard matrices (see [8]). In [15] Brierley and Weigert conducted an extensive search on all known Hadamard matrices in dimension 6 providing an impressive study of their biunimodular vectors leading to an approximate solution of the MUB problem in this dimension (for lower dimensions accessed via biunimodular vectors see [16]).

In the following sections we explain that the existence of biunimodular vectors for an arbitrary unitary matrix allows to understand the structure of unitary matrices in fairly simple terms.

2 Synthesis of $U(n)$

Unitary $n \times n$ matrices form the unitary group $U(n)$ and are a basic notion in mathematics, physics, chemistry and engineering. These matrices can be obtained in various standard ways: Gram-Schmidt process, Householder reflections, Hurwitz parametrization, Cayley transform and via Hermitian matrices using the matrix exponential. In 1952 Mur-naghan described a convenient parametrization of the unitary group (see [42]).³ This has been followed by the work of Reck *et al.* who in 1994 proved that any unitary matrix can be obtained as a sequence of consecutive beam splitter transformations, that can be conducted experimentally in the laboratory using optical devices ([45]). In the current century the research on finding the ways to generate unitary matrices has intensified. Nemoto described the special unitary group $SU(n)$ in [43] basing on an earlier result [46] of Rowe *et al.* Tilma and Sudarshan provided an Euler angle parametrization for $SU(n)$ and $U(n)$ (see [50, 51]). Meanwhile Diță in [25] has shown another description of $U(n)$. A recursive parametrization

³Another such parametrization has been provided in 1982 by Diță (see [24]).

of unitary matrices has been given by Jarlskog in [38] and a composite parameterization was done in [48] (see [17, 25] and [48] for more details on these developments).

The search for biunimodular vectors for an arbitrary unitary matrix can be motivated by the following recipe to generate unitary matrices. Consider $n \in \mathbb{N}$ and a set of n^2 complex parameters $\{a_{jk} \in \mathbb{T} : j, k = 1, 2, \dots, n\}$, where $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$. In order to synthesize a unitary matrix $A_n \in U(n)$ from these parameters, it is convenient to organize them as in the table below

a_{11}	a_{12}	a_{13}	\dots	a_{1n}
a_{21}	a_{22}	a_{23}	\dots	a_{2n}
a_{31}	a_{32}	a_{33}	\dots	a_{3n}
\vdots	\vdots	\vdots		\vdots
a_{n1}	a_{n2}	a_{n3}	\dots	a_{nn}

and run the following recursive procedure using the Fourier transform $(F_l)_{j,k} = \frac{1}{\sqrt{l}} e^{-2\pi i \frac{jk}{l}}$ and its conjugate transpose $(F_l^*)_{j,k} = \frac{1}{\sqrt{l}} e^{2\pi i \frac{jk}{l}}$.

The initial unitary matrix A_1 is given as $[a_{11}]$. And, in general, for $2 \leq l \leq n$

$$A_l = \begin{bmatrix} a_{l1} & 0 & \dots & 0 \\ 0 & a_{l2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_{ll} \end{bmatrix} F_l \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & \boxed{A_{l-1}} & & \\ \vdots & & & \\ 0 & & & \end{bmatrix} F_l^* \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & a_{l1} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_{l-1l} \end{bmatrix}, \quad (3)$$

with an obvious block matrix notation.

The above procedure is not one-to-one, meaning that different sets of parameters may give the same matrix. As to the question if it is onto, the simplicity of the above scheme can raise some doubts whether it can reveal the structure of an arbitrary unitary matrix. Nevertheless, in the next section we shall prove that all unitary matrices can be obtained in this way, provided that all of them possess biunimodular vectors.

3 Analysis of $U(n)$

We have the following basic

Proposition 3.1. *A unitary matrix $A \in U(n)$ has a biunimodular vector v if and only if*

$$A = \begin{bmatrix} w_1 & 0 & \dots & 0 \\ 0 & w_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & w_n \end{bmatrix} F_n \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & \boxed{B} & & \\ \vdots & & & \\ 0 & & & \end{bmatrix} F_n^* \begin{bmatrix} \overline{v_1} & 0 & \dots & 0 \\ 0 & \overline{v_2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \overline{v_n} \end{bmatrix},$$

where $v = (v_1, v_2, \dots, v_n) \in \mathbb{T}^n$, $Av = w = (w_1, w_2, \dots, w_n) \in \mathbb{T}^n$, B is some unitary matrix in $U(n-1)$ and F_n is the Fourier transform with the adjoint F_n^* .

Proof. We shall use the following notation. For an arbitrary vector $u \in \mathbb{C}^n$ by D_u we shall denote the diagonal matrix with u on the diagonal. We also consider the stabilizer group of u , defined as $\text{Fix}(u) = \{S \in U(n) : Su = u\}$ and let $\mathbf{1} = (1, 1, \dots, 1)$, $\mathbf{e} = (1, 0, \dots, 0)$ both in \mathbb{C}^n .

To conduct the proof we observe, that there exist unimodular vectors v and w such that $Av = w$ iff $AD_v \mathbf{1} = D_w \mathbf{1}$, what is equivalent to saying that $D_w^* A D_v \in \text{Fix}(\mathbf{1})$ with $v, w \in \mathbb{T}^n$.

The description of the group $\text{Fix}(\mathbf{1})$ is related to the group $\text{Fix}(\mathbf{e})$. Indeed, since $F_n \mathbf{e} = \frac{1}{\sqrt{n}} \mathbf{1}$, it is easy to see that $M \in \text{Fix}(\mathbf{1})$ iff $F_n^* M F_n \in \text{Fix}(\mathbf{e})$.

Therefore, we see that A has a biunimodular vector v iff $F_n^* D_w^* A D_v F_n \in \text{Fix}(\mathbf{e})$. Due to the obvious description of $\text{Fix}(\mathbf{e})$ the proposition follows. \square

Remark 3.2. *Clearly, if we can find a biunimodular vector v for A , then for every $c \in \mathbb{T}$ the vector cv is also biunimodular for A . Therefore, we can concentrate on biunimodular vectors with the leading entry v_1 equal to 1. This explains why Proposition 3.1 proves, that every unitary matrix can be obtained via formula (3) iff every unitary matrix has a biunimodular vector.*

Remark 3.3. *The Fourier transform F_n enters the above scheme as a generic unitary matrix with the property that $F_n \mathbf{e} = \frac{1}{\sqrt{n}} \mathbf{1}$. We need to clarify that, in the above proposition, F_n can be replaced by any unitary matrix F such that $F \mathbf{e} = \frac{1}{\sqrt{n}} \mathbf{1}$. However, clearly the easiest description of such F is given by $F = F_n M$ with $M \in \text{Fix}(\mathbf{e})$.*

In Section 10 we shall present an algorithm that for an explicitly given unitary matrix allows to search for its biunimodular vectors within a set precision. Therefore, in practice, a numerically given unitary matrix can be analysed to the point when all parameters $\{a_{jk} \in \mathbb{T} : j, k = 1, 2, \dots, n\}$ are found, that allow to synthesize the matrix back via formula (3).

On the other hand, as pointed out by the referees, one has the following crucial

Theorem 3.4. (Idel, Wolf + Biran, Entov, Polterovich) *Every unitary matrix has a biunimodular vector.*

This settles that scheme (3) for building unitary matrices gives all of them. The scheme has been discovered independently by De Vos and De Baerdemacker without the notion of biunimodular vectors. In [23] they conjectured that every unitary matrix U enjoys a LAR decomposition: $U = LAR$, where L and R are unitary diagonal matrices and A is a unitary doubly stochastic matrix, meaning that the row sums (and thus columns sums) of A are all equal to 1. This, clearly, is equivalent to saying that every unitary matrix U has a biunimodular vector and has been proved by Idel and Wolf in [36]. The proof relies on showing that the action of U on the torus \mathbb{T}^n defines a Hamiltonian symplectomorphism of the corresponding Clifford torus embeded in the complex projective space. The rest follows from [9], where Biran, Entov and Polterovich used Calabi quasimorphisms to prove that the Clifford torus cannot be displaced from itself by a Hamiltonian symplectomorphism. Idel and Wolf point also to the work [20] of Cho on Floer cohomology that one can combine with Theorem 3.4 to conclude, that every $n \times n$ unitary matrix has at least 2^{n-1} biunimodular vectors.

In the following section we shall examine the existence of biunimodular vectors from a few different angles.

4 Biunimodular problem

The biunimodular problem is to find (or prove the existence of) a biunimodular vector for a given unitary matrix. With the notation explained below we can restate this task in equivalent terms.

Theorem 4.1. *Let $A \in U(n)$. The matrix A has a biunimodular vector if and only if either of the following holds*

- (a) $A \in \mathcal{D} \cdot \text{Fix}(\mathbf{1}) \cdot \mathcal{D}_1$.
- (a') $A' \in \mathcal{D}' \cdot \text{E}(\mathbf{1}) \cdot \mathcal{D}'$.
- (b) $\|A\|_{\infty \rightarrow 1} = n$.

- (c) $\sup_{u \in \mathbb{T}^n} |\pi_A(u)| = 1$.
 (d) $A(\mathbb{T}^n) \cap \mathbb{T}^n \neq \emptyset$.

Proof.

(a) Here, $\mathcal{D} \subseteq U(n)$ denotes the subgroup of diagonal matrices with diagonal entries in \mathbb{T} , and $\mathcal{D}_1 \subseteq \mathcal{D}$ is the subgroup of matrices with the first diagonal entry equal to 1. $\text{Fix}(\mathbf{1}) = \{S \in U(n) : S\mathbf{1} = \mathbf{1}\}$, where $\mathbf{1} = (1, 1, \dots, 1) \in \mathbb{T}^n$. $A \in \mathcal{D} \cdot \text{Fix}(\mathbf{1}) \cdot \mathcal{D}_1$ means that A can be written as a product of three matrices from the indicated subgroups of $U(n)$. By Proposition 3.1 and Remark 3.2 this is equivalent to the existence of a biunimodular vector for A .

(a') Here, $A' = \lambda A$ with $\lambda^n = \overline{\det(A)}$, so $A' \in SU(n)$. $\mathcal{D}' = \mathcal{D} \cap SU(n)$ and $E(\mathbf{1})$ denotes the subgroup of $SU(n)$ that has $\mathbf{1}$ as an eigenvector. Clearly, (a') is a mere translation of (a) into the special unitary setting.

(b) Here, $\|A\|_{\infty \rightarrow 1} = \sup_{\|u\|_\infty=1} \|Au\|_1$ is the norm of $A : (\mathbb{C}^n, \|\cdot\|_\infty) \rightarrow (\mathbb{C}^n, \|\cdot\|_1)$, where the usual ℓ^p -norm of $u \in \mathbb{C}^n$ is given by $\|u\|_p = (\sum_{k=1}^n |u_k|^p)^{\frac{1}{p}}$ and $\|u\|_\infty = \sup_k |u_k|$.

For every $u \in \mathbb{C}^n$ we have $\|u\|_1 \leq \sqrt{n}\|u\|_2 \leq n\|u\|_\infty$. Therefore, for every $A \in U(n)$ we have

$$\|Au\|_1 \leq \sqrt{n}\|Au\|_2 = \sqrt{n}\|u\|_2 \leq n\|u\|_\infty, \quad (4)$$

proving that $\|A\|_{\infty \rightarrow 1} \leq n$. Thus, if A has a biunimodular vector v , then $\|Av\|_1 = n\|v\|_\infty$ showing that $\|A\|_{\infty \rightarrow 1} = n$.

Conversely, if $\|A\|_{\infty \rightarrow 1} = n$, compactness of the ℓ^∞ -ball implies the existence of a vector $u \in \mathbb{C}^n$ with $\|u\|_\infty = 1$ and $\|Au\|_1 = n\|u\|_\infty$. As the estimate (4) shows, this equality holds if and only if $\|Au\|_1 = \sqrt{n}\|Au\|_2$ and $\|u\|_2 = \sqrt{n}\|u\|_\infty$, meaning that both u and Au must be a constant multiple of a unimodular vector. Since $\|u\|_\infty = 1$ and $\|Au\|_1 = n$, both u and Au must be unimodular.

(c) Here, $\pi_A(u) = \pi(Au)$, where $\pi(u) = \prod_{k=1}^n u_k$ for $u \in \mathbb{C}^n$.

Let $A \in U(n)$, $u \in \mathbb{T}^n$ and $Au = w$. We have

$$|\pi_A(u)|^2 = \prod_{k=1}^n |w_k|^2 \leq \left(\frac{1}{n}\|w\|_2^2\right)^n = \left(\frac{1}{n}\|u\|_2^2\right)^n = 1, \quad (5)$$

so $|\pi_A(u)| \leq 1$. Thus, if A has a biunimodular vector v , then $|\pi_A(v)| = 1$ showing that $\sup_{u \in \mathbb{T}^n} |\pi_A(u)| = 1$.

Conversely, if $\sup_{u \in \mathbb{T}^n} |\pi_A(u)| = 1$, compactness of \mathbb{T}^n implies the existence of a vector $u \in \mathbb{T}^n$ with $|\pi_A(u)| = 1$. In light of (5) this means that $1 = \prod_{k=1}^n |w_k|^2 = \left(\frac{1}{n}\|w\|_2^2\right)^n$, i.e. $w = Au$ must be unimodular.

(d) Clearly, a vector v is biunimodular for $A \in U(n)$ iff $Av \in A(\mathbb{T}^n) \cap \mathbb{T}^n$, so the equivalence in this case is trivial. \square

Remark 4.2. Part (a) of Theorem 4.1 is equivalent to saying that $A \in \mathcal{D} \cdot \text{Fix}(\mathbf{1}) \cdot \mathcal{D}$. Thus, Theorem 3.4 is equivalent to the decomposition $U(n) = \mathcal{D} \cdot \text{Fix}(\mathbf{1}) \cdot \mathcal{D}$. Unfortunately, there is no general theory explaining when two subgroups H, H' of a Lie group G yield the decomposition $G = H \cdot H' \cdot H$. Moreover, the Cartan decomposition and Kostant decomposition of any semisimple Lie group G , that both are given in this form, indicate potential difficulties in developing such a general explanation.

For part (a') included in the above characterization, we would like to notice that \mathcal{D}' is a maximal torus subgroup of a compact simple Lie group $SU(n)$. Thus, Theorem 3.4 is equivalent to the following maximal torus decomposition:

$$SU(n) = \mathcal{D}' \cdot E(\mathbf{1}) \cdot \mathcal{D}',$$

with $\dim(SU(n)) = \dim(E(\mathbf{1})) + 2 \dim(\mathcal{D}')$. This allows to conjecture, or ask, whether every compact simple Lie group G admits a maximal torus decomposition $G = T \cdot H \cdot T$, with a maximal torus T of G and a subgroup $H \subseteq G$ such that $\dim G = \dim H + 2 \dim T$.

Regarding part (b), as in [31], an interpolation argument can be used to conclude that $\|A\|_{\infty \rightarrow 1} = n$ is in turn equivalent to saying that $\|A\|_{p \rightarrow q} = n^{\frac{1}{q} - \frac{1}{p}}$ in the region $1 \leq q \leq 2 \leq p \leq \infty$. This further amplifies the interest in biunimodular vectors, that are precisely those vectors, where the norm $\|A\|_{p \rightarrow q} = n^{\frac{1}{q} - \frac{1}{p}}$ is attained, in the indicated range of p and q .

Part (c) of the theorem is equivalent to $\sup_{u \in \mathbb{D}^n} |\pi_A(u)| = 1$, where $\mathbb{D} = \{z \in \mathbb{C} : |z| \leq 1\}$. Thus, the biunimodular problem can be viewed as an extremum problem for the modulus of a polynomial $\pi_A : \mathbb{D}^n \rightarrow \mathbb{D}$.

Part (d) of the characterization provides a deceptively simple geometric interpretation of the problem: Describe the intersection of two tori. This geometric angle has been exploited to prove Theorem 3.4.

With the above characterization we close the motivational part of the paper and present our findings on the biunimodular problem.

5 $U(2)$

Obtaining biunimodular vectors of a given unitary 2×2 matrix is an easy task.

Proposition 5.1. *Every matrix in $U(2)$ has a biunimodular vector.*

Proof. Every matrix $A \in U(2)$ can be written as

$$A = \begin{bmatrix} x & y \\ -z\bar{y} & z\bar{x} \end{bmatrix},$$

with $z \in \mathbb{T}$ and $x, y \in \mathbb{C}$ such that $|x|^2 + |y|^2 = 1$. Finding a biunimodular vector $(1, d)$ for A amounts to solving a system of two equations: $|x + yd| = 1$ and $|\bar{y} - \bar{x}d| = 1$. Since $|x|^2 + |y|^2 = |d| = 1$ the system is equivalent to the equation $\operatorname{Re}(\bar{x}yd) = 0$. Therefore, we see that if $xy = 0$ then every vector $(1, d)$ with $d \in \mathbb{T}$ is biunimodular for A . While for $xy \neq 0$ the matrix A has precisely two biunimodular vectors with the leading 1 entry:

$$(1, ie^{i(\alpha-\beta)}), \quad (1, -ie^{i(\alpha-\beta)}), \quad (6)$$

where $\alpha = \arg x$ and $\beta = \arg y$. \square

As we indicated in Section 2, the existence of biunimodular vectors for every matrix in $U(2)$ allows for writing an alternative formula describing $U(2)$.

Corollary 5.2.

$$U(2) = \left\{ \frac{1}{2} \begin{bmatrix} a(1+z) & ac(1-z) \\ b(1-z) & bc(1+z) \end{bmatrix} : a, b, c, z \in \mathbb{T} \right\} \quad (7)$$

Proof. Let $A \in U(2)$. Since A has a biunimodular vector, by Theorem 4.1 we have that $A \in \mathcal{D} \cdot \operatorname{Fix}(\mathbf{1}) \cdot \mathcal{D}_1$. Clearly, in this case

$$\operatorname{Fix}(\mathbf{1}) = \left\{ \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & z \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} : z \in \mathbb{T} \right\} = \left\{ \frac{1}{2} \begin{bmatrix} 1+z & 1-z \\ 1-z & 1+z \end{bmatrix} : z \in \mathbb{T} \right\},$$

and therefore

$$A = \frac{1}{2} \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \begin{bmatrix} 1+z & 1-z \\ 1-z & 1+z \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & c \end{bmatrix},$$

with $a, b, c, z \in \mathbb{T}$ as desired. \square

To close this section we point out that the above observations follow, as well, from writing an arbitrary matrix in $U(2)$ as $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \begin{bmatrix} \cos \varphi & \sin \varphi \\ -\sin \varphi & \cos \varphi \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & c \end{bmatrix}$ with some $a, b, c \in \mathbb{T}$, $\varphi \in [0, 2\pi]$ and noting that $\begin{bmatrix} \cos \varphi & \sin \varphi \\ -\sin \varphi & \cos \varphi \end{bmatrix} = \frac{e^{-i\varphi}}{2} \begin{bmatrix} 1 & 0 \\ 0 & -i \end{bmatrix} \begin{bmatrix} 1+z & 1-z \\ 1-z & 1+z \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$ with $z = e^{i2\varphi}$.

6 $U(3)$

Some elementary calculations allow to conclude that all orthogonal matrices in $O(3)$ have a biunimodular vector. Another easy case is given in the following.

Example 6.1. *For $A \in U(3)$ with at least one zero entry we shall explain how to exhibit its biunimodular vectors. By interchanging rows and columns of A we can assume that there is a zero entry in the top right corner of A . Moreover, we can multiply rows and columns of A by unimodular constants in such a way that the outcome shall have only real entries. Therefore, we can assume that A is given as*

$$\begin{bmatrix} \cos \alpha & \sin \alpha & 0 \\ x \sin \alpha & -x \cos \alpha & y \\ y \sin \alpha & -y \cos \alpha & -x \end{bmatrix}$$

with $\alpha \in [0, 2\pi]$ and $x, y \in \mathbb{R}$ such that $x^2 + y^2 = 1$. A simple check reveals that such a matrix has at least four distinct biunimodular vectors with the leading 1 entry:

$$(1, i, e^{i\alpha}), \quad (1, -i, e^{-i\alpha}), \quad (1, i, -e^{i\alpha}), \quad (1, -i, -e^{-i\alpha}).$$

Moreover, if A has only one zero entry, then there are no other biunimodular vectors for A . It is also clear, that when A has at least two zero entries, then at least one of its entries has modulus 1 leading to a trivialization of A and a continuum of biunimodular vectors.

Remark 6.2. *Whenever we talk about the number of biunimodular vectors for a given unitary matrix, we concentrate only on vectors with the leading entry equal to 1, as it was indicated in Remark 3.2. The above example explains the structure and the number of biunimodular vectors for $A \in U(3)$ in the case when A has at least one zero entry. In the case when all entries of $A \in U(3)$ are nonzero, we have only found examples of matrices with the number of biunimodular vectors equal to 4, 5 or 6.*

In order to exhibit the method allowing to count biunimodular vectors of a given matrix $A \in U(3)$, let us consider a vector $u = u_{xy} = (1, e^{ix}, e^{iy})$ and the square $Q = [-\pi, \pi]^2$. The idea is to look at three regions $R_j = \{(x, y) \in Q : |Au(j)| \geq 1\}$, $j = 1, 2, 3$ and check the intersection of their boundaries.

For the Fourier case $A = F_3$ the corresponding three regions are given in Fig.1. The points where the boundaries of these regions intersect correspond to biunimodular vectors of A . From the unitarity of A it follows that every intersection point of two such boundaries belongs to the boundary of the third region as well, allowing for a visual count of biunimodular vectors. The next figure shows these regions for three exemplary unitary matrices providing the mentioned count of biunimodular vectors (conducted and plotted with *Mathematica*).

In general, since A is unitary these closed regions cover Q , and therefore, any of these regions must intersect with at least one of the two other regions. Unfortunately, it is hard to argue that at least one pair of the regions intersects in such a way that their boundaries also intersect, closing a natural way to prove Theorem 6.3. This obstacle boils down to the lack of proof for a classification of the regions R_j , that essentially can be simplified to

$$E_{st} = \{(x, y) \in Q : s \cos(x) + t \cos(y) + \cos(x - y) \geq 0\}, \quad s, t > 0$$

and are hard to study.

A working proof that all $A \in U(3)$ have biunimodular vectors, that we give below, relies on findings of Section 8, that are included in Appendix A.

Theorem 6.3. *Every matrix in $U(3)$ has a biunimodular vector.*

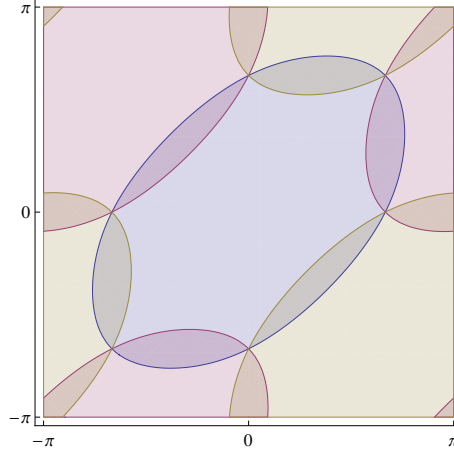


Figure 1: The regions R_j , $j = 1, 2, 3$ for the Fourier case F_3 .

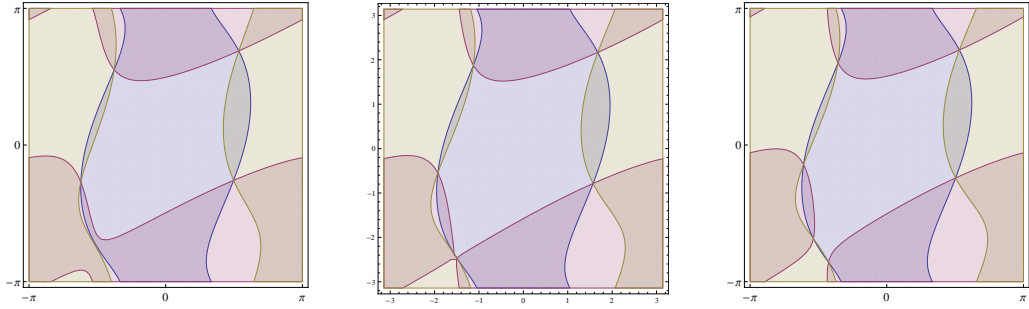


Figure 2: Counting biunimodular vectors in dimension $n = 3$.

Proof. In Appendix A (Observation A.3) we prove that

$$U(3) = \{\text{diag}(\lambda_1, \lambda_2, \lambda_3) T_{(\alpha, \beta, \gamma, z)} \text{diag}(1, \lambda_4, \lambda_5) : \alpha, \beta, \gamma \in [0, 2\pi]; z, \lambda_j \in \mathbb{T}, j = 1, \dots, 5\},$$

where

$$T_{(\alpha, \beta, \gamma, z)} = \begin{bmatrix} \cos \alpha & -\sin \alpha \sin \gamma & \sin \alpha \cos \gamma \\ -\sin \alpha \sin \beta & z \cos \beta \cos \gamma - \cos \alpha \sin \beta \sin \gamma & z \cos \beta \sin \gamma + \cos \alpha \sin \beta \cos \gamma \\ \sin \alpha \cos \beta & z \sin \beta \cos \gamma + \cos \alpha \cos \beta \sin \gamma & z \sin \beta \sin \gamma - \cos \alpha \cos \beta \cos \gamma \end{bmatrix}.$$

Thus, in order to prove that every matrix in $U(3)$ has a biunimodular vector, it is enough to show it for the matrix $T_{(\alpha, \beta, \gamma, z)}$.

Therefore, we want to find $x, y \in \mathbb{R}$ such that $T_{(\alpha, \beta, \gamma, z)}$ applied to the vector $(1, e^{ix}, e^{iy})$ yields a unimodular outcome $v \in \mathbb{T}^3$. The first entry of this outcome is given by $\cos \alpha + w \sin \alpha$ with $w = -e^{ix} \sin \gamma + e^{iy} \cos \gamma$. By applying $\begin{bmatrix} \cos \alpha & \sin \alpha \\ \sin \alpha & -\cos \alpha \end{bmatrix}$ to $(1, w)$, we see that $|\cos \alpha + w \sin \alpha| = 1$ iff $|w| = |\sin \alpha - w \cos \alpha|$ iff $\sin \alpha - w \cos \alpha = e^{im} w$ for some $m \in \mathbb{R}$. Thus, we can add m as another variable to our problem and require that $\sin \alpha - w \cos \alpha = e^{im} w$.

Then, the second entry of v is given as $v_2 = uz \cos \beta - e^{im} w \sin \beta$, where $u = e^{ix} \cos \gamma + e^{iy} \sin \gamma$. And $v_3 = uz \sin \beta + e^{im} w \cos \beta$. In short,

$$\begin{bmatrix} v_2 \\ v_3 \end{bmatrix} = \begin{bmatrix} \cos \beta & -\sin \beta \\ \sin \beta & \cos \beta \end{bmatrix} \begin{bmatrix} z & 0 \\ 0 & e^{im} \end{bmatrix} \begin{bmatrix} \cos \gamma & \sin \gamma \\ -\sin \gamma & \cos \gamma \end{bmatrix} \begin{bmatrix} e^{ix} \\ e^{iy} \end{bmatrix} := U_m \begin{bmatrix} e^{ix} \\ e^{iy} \end{bmatrix} \quad (8)$$

and we need to find $x, y, m \in \mathbb{R}$ such that $|v_2| = |v_3| = 1$ and $\sin \alpha - w \cos \alpha = e^{im} w$, with $w = -e^{ix} \sin \gamma + e^{iy} \cos \gamma$. Since (8) reads $U_m(e^{ix}, e^{iy}) \in \mathbb{T}^2$ with $U_m \in U(2)$, we can recognize the task of finding x, y, m as a biunimodular problem with a certain twist.

By looking at (6) we can simplify the above problem. Indeed, by Proposition 5.1, for every $m \in \mathbb{R}$ we can find at least two vectors $(1, \pm i e^{i\varphi_m})$ such that $U_m(1, \pm i e^{i\varphi_m}) \in \mathbb{T}^2$, giving $|v_2| = |v_3| = 1$. Thus, let us consider

$$w_j(m) = -\sin \gamma + (-1)^j i e^{i\varphi_m} \cos \gamma$$

with $j = 1, 2$ and concentrate on the final equation $\sin \alpha - w_j(m) \cos \alpha = e^{im} w_j(m)$.

Clearly, if $|\cos \alpha| = 1$, then the matrix $T_{(\alpha, \beta, \gamma, z)}$ is simple enough to have a biunimodular vector, see Remark 6.1. Hence, we assume $|\cos \alpha| < 1$ and claim that (8) has a desired solution $x, y, m \in \mathbb{R}$, as long as we can find $m_0 \in \mathbb{R}$ and $j_0 \in \{1, 2\}$ such that

$$|w_{j_0}(m_0)| = \left| \frac{\sin \alpha}{e^{im_0} + \cos \alpha} \right| \quad (9)$$

Indeed, after establishing a solution to (9), we can find $x_0 \in \mathbb{R}$ such that

$$e^{ix_0} w_{j_0}(m_0) = \frac{\sin \alpha}{e^{im_0} + \cos \alpha},$$

so $\sin \alpha - e^{ix_0} w_{j_0}(m_0) \cos \alpha = e^{im_0} w_{j_0}(m_0)$, leading to the conclusion that m_0, j_0 and x_0 solve (8) by setting $(e^{ix}, e^{iy}) = e^{ix_0}(1, (-1)^{j_0} i e^{i\varphi_{m_0}})$.

Thus, we are left with solving (9). Here, it is important to notice that the biunimodular vectors $(1, i e^{i\varphi_m})$ and $(1, -i e^{i\varphi_m})$ are orthogonal. Thus, if we define $f_j(m) = |w_j(m)|^2$ for $j = 1, 2$ and $m \in [0, 2\pi]$, then $f_1(m) + f_2(m) = 2\|(-\sin \gamma, \cos \gamma)\|_2^2 = 2$. Moreover, there is an $m_1 \in [0, 2\pi]$ such that $e^{im_1} = z$, and then $\varphi_{m_1} = 0$ by (6), so $f_1(m_1) = f_2(m_1) = 1$.

Finally, let us notice that for $g(m) = \left| \frac{\sin \alpha}{e^{im} + \cos \alpha} \right|^2$ one has $\inf g = \left(\frac{|\sin \alpha|}{1 + |\cos \alpha|} \right)^2 \leq 1$ and $\sup g = \left(\frac{|\sin \alpha|}{1 - |\cos \alpha|} \right)^2 \geq 1$.

This allows to finish the proof. Indeed, if $f_1 > g$ and $f_2 > g$, then $1 > g$ contradicting $\sup g \geq 1$. Similarly, if $f_1 < g$ and $f_2 < g$, then $1 < g$ contradicting $\inf g \leq 1$. Thus, there is an $m_2 \in [0, 2\pi]$ such that $g(m_2)$ is between $f_1(m_2)$ and $f_2(m_2)$. However, g can not be strictly between f_1 and f_2 on $[0, 2\pi]$, because $f_1(m_1) = f_2(m_1)$. Therefore, there is an $m_0 \in [0, 2\pi]$ such that either $g(m_0) = f_1(m_0)$ or $g(m_0) = f_2(m_0)$. \square

Remark 6.4. Since for any vector $R \in \mathbb{C}^n$ with $\|R\|_2 = 1$ the average $\int_{\mathbb{T}^n} |\langle R, u \rangle|^2 du$ is equal to one, it is easy to see, that for such R there is a $u \in \mathbb{T}^n$, such that $|\langle R, u \rangle| = 1$.

For two orthonormal vectors $R_1, R_2 \in \mathbb{C}^n$ finding a vector $u \in \mathbb{T}^n$ such that $|\langle R_1, u \rangle| = |\langle R_2, u \rangle| = 1$ seems to be a much harder task, and Theorem 6.3 is equivalent to accomplishing this task with $n = 3$. Currently, the only arguments extending this property for $n \geq 4$ rely on Theorem 3.4. For orthonormal $R_1, R_2 \in \ell^1(\mathbb{Z}) \subset \ell^2(\mathbb{Z})$ the problem is open.

As in the $U(2)$ case, the existence of biunimodular vectors for all members of $U(3)$ allows to write a formula for an arbitrary matrix in $U(3)$.

Corollary 6.5. $A \in U(3)$ if and only if

$$A = \frac{1}{6} \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 1 & \bar{\omega} & \omega \\ 1 & \omega & \bar{\omega} \end{bmatrix} \begin{bmatrix} 2 & 0 & 0 \\ 0 & a(1+z) & ac(1-z) \\ 0 & b(1-z) & bc(1+z) \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \bar{\omega} \\ 1 & \bar{\omega} & \omega \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & \lambda_4 & 0 \\ 0 & 0 & \lambda_5 \end{bmatrix}$$

for some parameters $a, b, c, z, \lambda_j \in \mathbb{T}$, $j = 1, \dots, 5$ and $\omega = e^{\frac{2\pi i}{3}}$.

Proof. Let $A \in U(3)$. By Theorems 6.3 and 4.1 we have that $A \in \mathcal{D} \cdot \text{Fix}(\mathbf{1}) \cdot \mathcal{D}_1$. Moreover, in this case $\text{Fix}(\mathbf{1}) = F_3 \cdot \text{Fix}((1, 0, 0)) \cdot F_3^*$, where F_3 is the Fourier transform and

$$\text{Fix}((1, 0, 0)) = \left\{ \frac{1}{2} \begin{bmatrix} 2 & 0 & 0 \\ 0 & a(1+z) & ac(1-z) \\ 0 & b(1-z) & bc(1+z) \end{bmatrix} : a, b, c, z \in \mathbb{T} \right\}$$

due to the description of $U(2)$ provided in Corollary 5.2. Since $F_3 = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & 1 & 1 \\ 1 & \bar{\omega} & \omega \\ 1 & \omega & \bar{\omega} \end{bmatrix}$ we can finish the proof. \square

Moreover, as a byproduct from the proof of Theorem 6.3 we obtain the following description of $U(3)$.

Corollary 6.6.

$$\begin{aligned} U(3) &= \{ \text{diag}(\lambda_1, \lambda_2, \lambda_3) X_\beta Y_\alpha^z X_\gamma \text{diag}(1, \lambda_4, \lambda_5) : \alpha, \beta, \gamma \in [0, 2\pi]; z, \lambda_j \in \mathbb{T}, j = 1, \dots, 5 \} \\ &= \{ \text{diag}(\lambda_1, \lambda_2, \lambda_3) Z_\beta Y_\alpha^z X_\gamma \text{diag}(1, \lambda_4, \lambda_5) : \alpha, \beta, \gamma \in [0, 2\pi]; z, \lambda_j \in \mathbb{T}, j = 1, \dots, 5 \}, \end{aligned}$$

where for a given $\varphi \in [0, 2\pi]$

$$X_\varphi = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos \varphi & -\sin \varphi \\ 0 & \sin \varphi & \cos \varphi \end{bmatrix}, \quad Y_\varphi^z = \begin{bmatrix} \cos \varphi & 0 & -\sin \varphi \\ 0 & z & 0 \\ \sin \varphi & 0 & \cos \varphi \end{bmatrix}, \quad Z_\varphi = \begin{bmatrix} \cos \varphi & -\sin \varphi & 0 \\ \sin \varphi & \cos \varphi & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Proof. This follows from Observation A.3 used in the proof of Theorem 6.3 and the matrix factorization:

$$T_{(\alpha, \beta, \gamma, z)} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos \beta & -\sin \beta \\ 0 & \sin \beta & \cos \beta \end{bmatrix} \begin{bmatrix} \cos \alpha & 0 & -\sin \alpha \\ 0 & z & 0 \\ \sin \alpha & 0 & \cos \alpha \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos \gamma & \sin \gamma \\ 0 & \sin \gamma & -\cos \gamma \end{bmatrix},$$

that leads to the provided description of $U(3)$ via easy matrix manipulations. \square

The above description of $U(3)$ can be compared with the standard Euler-Tait-Bryan decomposition of $O(3)$:

$$O(3) = \{ X_\beta Y_\alpha^z X_\gamma : \alpha, \beta, \gamma \in [0, 2\pi]; z = \pm 1 \} = \{ Z_\beta Y_\alpha^z X_\gamma : \alpha, \beta, \gamma \in [0, 2\pi]; z = \pm 1 \}.$$

7 $U(4)$ and beyond

The study conducted in the two previous sections allows to surmise that, excluding some trivial cases, the number of biunimodular vectors for $A \in U(n)$ is finite when $n \leq 3$. The classic example of the Fourier transform F_4 indicates a crucial change in the amount of biunimodular vectors, when $n \geq 4$. To understand this phenomenon it is enough to notice that $(1, 0, 1, 0)$ and $(0, 1, 0, -1)$ are eigenvectors of F_4 . Thus, $(1, z, 1, -z)$ is biunimodular for F_4 for all $z \in \mathbb{T}$. An investigation of the remaining biunimodular vectors for F_4 , that are given as $(1, z, -1, z)$, allows to see a pattern that guarantees a continuum of biunimodular vectors.

In order to view this pattern, for $u \in \mathbb{C}^n$ we define its support as $\text{supp}(u) = \{k \in \{1, 2, \dots, n\} : u_k \neq 0\}$ and consider the following.

Observation 7.1. *Let $A \in U(n)$. If there are $u, w \in \mathbb{C}^n$ such that each of the vectors $|u|, |w|, |Au|, |Aw|$ is equal to 1 on its support and both disjoint unions $\text{supp}(u) \cup \text{supp}(w) = \text{supp}(Au) \cup \text{supp}(Aw)$ cover $\{1, 2, \dots, n\}$, then $u + zw$ is biunimodular for A for all $z \in \mathbb{T}$.*

The above observation allows to construct matrices in $U(n)$ with all nonzero entries having a continuum of biunimodular vectors, whenever $n \geq 4$. It also allows for a further appreciation of Haagerup's result stated in Theorem 1.2. It is not clear, however, whether for all unitary matrices with a continuum of biunimodular vectors one can find vectors u and w as in Observation 7.1. Even if this would be true, pointing to a conclusion that for any unitary matrix the set of its biunimodular vectors is a (finite) union of tori, it still would not tell, whether the set can be empty or not, underscoring the importance of Theorem 3.4.

In the next section, we provide an alternative way of building $U(2^n)$, that is based solely on the biunimodular structure of $U(2)$. After that, we conduct the study of biunimodular vectors in the general $U(n)$ case from the Lie groups perspective. Finally, we present a numerical treatment of the biunimodular problem with certain applications to the classical Fourier case.

8 $U(2^n)$

In this section we show, that a further generalization of the biunimodular problem allows to build all matrices in $U(2n)$ from matrices in $U(n)$.

In order to achieve this goal we employ the formula for $U(2)$ given in Section 5:

$$U(2) = \left\{ \frac{1}{2} \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \begin{bmatrix} 1+z & 1-z \\ 1-z & 1+z \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & c \end{bmatrix} : a, b, c, z \in \mathbb{T} \right\} \quad (10)$$

and replace the unimodular numbers $a, b, c, z \in \mathbb{T}$ by unitary matrices $A, B, C, Z \in U(n)$.

Theorem 8.1. *For every $n \in \mathbb{N}$*

$$U(2n) = \left\{ \frac{1}{2} \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix} \begin{bmatrix} I+Z & I-Z \\ I-Z & I+Z \end{bmatrix} \begin{bmatrix} I & 0 \\ 0 & C \end{bmatrix} : A, B, C, Z \in U(n) \right\}, \quad (11)$$

where I stands for the identity matrix in $U(n)$.

The above theorem yields immediately a map from \mathbb{T}^{4^n} onto $U(2^n)$ via an obvious inductive procedure starting from the trivial map from \mathbb{T} onto $U(1)$. In the first step of this procedure we recover (10). In the next step we get a formula for $U(4)$ that is enclosed in Appendix A.

Before we prove the theorem, we need a slim primary on block matrices. Let $M(n)$ denote the set of all $n \times n$ matrices with complex entries. An arbitrary matrix in $M(2n)$ can be written in a block form as $\begin{bmatrix} A & B \\ C & D \end{bmatrix}$ with $A, B, C, D \in M(n)$.

Clearly, we have that $\begin{bmatrix} A & B \\ C & D \end{bmatrix} \begin{bmatrix} A' & B' \\ C' & D' \end{bmatrix} = \begin{bmatrix} AA' + BC' & AB' + BD' \\ CA' + DC' & CB' + DD' \end{bmatrix}$ and $\begin{bmatrix} A & B \\ C & D \end{bmatrix}^* = \begin{bmatrix} A^* & C^* \\ B^* & D^* \end{bmatrix}$. Moreover, every $2n \times n$ matrix with complex entries can be written as $\begin{bmatrix} X \\ Y \end{bmatrix}$ with $X, Y \in M(n)$ and $\begin{bmatrix} A & B \\ C & D \end{bmatrix} \begin{bmatrix} X \\ Y \end{bmatrix} = \begin{bmatrix} AX + BY \\ CX + DY \end{bmatrix}$.

Lemma 8.2. *Let $\frac{1}{\sqrt{2}} \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in U(2n)$ with $A \in U(n)$ and $B, C, D \in M(n)$. Then $B, C, D \in U(n)$.*

Proof. Let $U = \frac{1}{\sqrt{2}} \begin{bmatrix} A & B \\ C & D \end{bmatrix}$ and $I \in U(n)$ be the identity matrix. Since $UU^* = \begin{bmatrix} I & 0 \\ 0 & I \end{bmatrix}$ we get that $BB^* = I$. Considering $U^*U = \begin{bmatrix} I & 0 \\ 0 & I \end{bmatrix}$ yields that $C^*C = I$ and $D^*D = I$. \square

Proof of Theorem 8.1. We can recognize the task as a special sort of a biunimodular problem. For an arbitrary unitary matrix $U \in U(2n)$ we need to find a unitary matrix $C \in U(n)$ such that $U \begin{bmatrix} I \\ C^* \end{bmatrix}$ is “unimodular”, in the sense that

$$U \begin{bmatrix} I \\ C^* \end{bmatrix} = \begin{bmatrix} A \\ B \end{bmatrix} \text{ with } A, B, C \in U(n). \quad (12)$$

(The general biunimodular problem of finding $A, B, C, D \in U(n)$ such that $U \begin{bmatrix} D^* \\ C^* \end{bmatrix} = \begin{bmatrix} A \\ B \end{bmatrix}$ collapses to the latter since $U \begin{bmatrix} D^* \\ C^* \end{bmatrix} = \begin{bmatrix} A \\ B \end{bmatrix}$ iff $U \begin{bmatrix} I \\ C^*D \end{bmatrix} = \begin{bmatrix} AD \\ BD \end{bmatrix}$.) Therefore, the goal is to repeat the arguments used in Section 5, carefully replacing the unimodular numbers in \mathbb{T} by unitary matrices in $U(n)$.

We start by noting that solving (12) amounts to saying that $\begin{bmatrix} A^* & 0 \\ 0 & B^* \end{bmatrix} U \begin{bmatrix} I & 0 \\ 0 & C^* \end{bmatrix} \begin{bmatrix} I \\ I \end{bmatrix} = \begin{bmatrix} I \\ I \end{bmatrix}$, i.e. that $V = \begin{bmatrix} A^* & 0 \\ 0 & B^* \end{bmatrix} U \begin{bmatrix} I & 0 \\ 0 & C^* \end{bmatrix}$ belongs to $\text{Fix} \begin{bmatrix} I \\ I \end{bmatrix} = \left\{ V \in U(2n) : V \begin{bmatrix} I \\ I \end{bmatrix} = \begin{bmatrix} I \\ I \end{bmatrix} \right\}$. The description of the group $\text{Fix} \begin{bmatrix} I \\ I \end{bmatrix}$ is again related to $\text{Fix} \begin{bmatrix} I \\ 0 \end{bmatrix} = \left\{ \begin{bmatrix} I & 0 \\ 0 & Z \end{bmatrix} : Z \in U(n) \right\}$ since $\mathbb{F} = \frac{1}{\sqrt{2}} \begin{bmatrix} I & I \\ I & -I \end{bmatrix} \in U(2n)$ and $\mathbb{F} \begin{bmatrix} I \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} I \\ I \end{bmatrix}$. Thus, $V \in \text{Fix} \begin{bmatrix} I \\ I \end{bmatrix}$ iff $\mathbb{F}V\mathbb{F} \in \text{Fix} \begin{bmatrix} I \\ 0 \end{bmatrix}$, being in turn equivalent to $V = \mathbb{F} \begin{bmatrix} I & 0 \\ 0 & Z \end{bmatrix} \mathbb{F} = \frac{1}{2} \begin{bmatrix} I+Z & I-Z \\ I-Z & I+Z \end{bmatrix}$ with some $Z \in U(n)$.

In this way we get that

$$U = \frac{1}{2} \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix} \begin{bmatrix} I+Z & I-Z \\ I-Z & I+Z \end{bmatrix} \begin{bmatrix} I & 0 \\ 0 & C \end{bmatrix},$$

for some $A, B, C \in U(n)$ iff (12) holds.

In order to solve the biunimodular problem (12) we write $U = \begin{bmatrix} X & Y \\ X' & Y' \end{bmatrix}$ with $X, Y, X', Y' \in M(n)$ and apply the singular value decomposition (SVD) to X and Y .

Recall that for an arbitrary matrix $M \in M(n)$ there are unitary matrices $W, W' \in U(n)$ and a diagonal matrix with non-negative entries $\Sigma \in M(n)$ such that $M = W'\Sigma W^*$. This leads to the polar decomposition $M = S_M U_M$ with $S_M = W'\Sigma(W')^*$ - a positive semi-definite matrix and a unitary matrix $U_M = W'W^* \in U(n)$.

In short, we use polar decomposition $X = S_X U_X$, $Y = S_Y U_Y$ to write

$$U = \begin{bmatrix} S_X U_X & S_Y U_Y \\ X' & Y' \end{bmatrix}$$

and claim that

$$U \begin{bmatrix} I \\ iU_Y^* U_X \end{bmatrix} = \begin{bmatrix} A \\ B \end{bmatrix}$$

with $A, B \in U(n)$ as desired, so $C^* = iU_Y^* U_X$ solves problem (12). To see this, we check that $A = (S_X + iS_Y)U_X$ and $AA^* = S_X^2 + S_Y^2 + i(S_Y S_X - S_X S_Y)$. Since $UU^* = \begin{bmatrix} I & 0 \\ 0 & I \end{bmatrix}$ we get that $S_X^2 + S_Y^2 = I$, so S_X^2 and S_Y^2 commute. For positive semi-definite matrices S_X and S_Y this means that they commute as well and, therefore, $A \in U(n)$.

To finish the proof we make the final observation that $A \in U(n)$ already implies that $B \in U(n)$. Indeed, we can extend the matrix $\frac{1}{\sqrt{2}} \begin{bmatrix} I \\ C^* \end{bmatrix}$ to a unitary matrix $\frac{1}{\sqrt{2}} \begin{bmatrix} I & C \\ C^* & -I \end{bmatrix} \in U(2n)$ and see that $\frac{1}{\sqrt{2}} U \begin{bmatrix} I & C \\ C^* & -I \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} A & X'' \\ B & Y'' \end{bmatrix} \in U(2n)$. Since A is unitary, Lemma 8.2 assures that $B \in U(n)$.

Therefore, we have proved that every $U \in U(2n)$ can be written in the way prescribed by (11). On the other hand, we have already checked that $\mathbb{F} \begin{bmatrix} I & 0 \\ 0 & Z \end{bmatrix} \mathbb{F} = \frac{1}{2} \begin{bmatrix} I+Z & I-Z \\ I-Z & I+Z \end{bmatrix} \in U(2n)$ for an arbitrary $Z \in U(n)$, so formula (11) holds. \square

9 $U(n)$

We are interested in finding the biunimodular vectors associated to a matrix $A \in U(n)$ for any $n \in \mathbb{N}$. As it was pointed out in Remark 3.2 we can concentrate on biunimodular vectors with the leading entry equal to 1. Let us denote the collection of such vectors as $\text{Bi}(A)$, so

$$\text{Bi}(A) = \{(v_1, v_2, \dots, v_n) \in \mathbb{T}^n \cap A^*(\mathbb{T}^n) : v_1 = 1\}.$$

Moreover, let us make the following formal definition:

$$\mathcal{B}_n = \{A \in U(n) : \text{Bi}(A) \neq \emptyset\}.$$

Clearly, \mathcal{B}_n is the set of $n \times n$ unitary matrices that possess biunimodular vectors and Theorem 3.4 asserts that $\mathcal{B}_n = U(n)$. While it would be hard to reproduce this result, one can check what information about \mathcal{B}_n and $\text{Bi}(A)$ can be drawn by using basic tools of Lie groups theory.

9.1 The main correspondence

The main tool for understanding \mathcal{B}_n and $\text{Bi}(A)$ will be the factorization conducted in Proposition 3.1. As we noticed in Theorem 4.1(a) the proposition implies that $A \in \mathcal{B}_n$ iff $A \in \mathcal{D} \cdot \text{Fix}(\mathbf{1}) \cdot \mathcal{D}_1$, where $\mathcal{D} \subseteq U(n)$ denotes the subgroup of diagonal matrices with diagonal entries in \mathbb{T} , $\mathcal{D}_1 \subseteq \mathcal{D}$ is the subgroup of matrices with the first diagonal entry equal to 1 and $\text{Fix}(\mathbf{1}) = \{S \in U(n) : S\mathbf{1} = \mathbf{1}\}$ with $\mathbf{1} = (1, 1, \dots, 1) \in \mathbb{C}^n$ is also a subgroup of $U(n)$. This allows to consider the following map

$$\Phi : \mathcal{D} \times \text{Fix}(\mathbf{1}) \times \mathcal{D}_1 \rightarrow U(n)$$

$$\Phi(D_1, S, D_2) = D_1 S D_2$$

containing the entire information concerning the existence of biunimodular vectors.

Indeed, the matrices possessing biunimodular vectors are given as the image of Φ , what already provides some information on \mathcal{B}_n .

Proposition 9.1. $\mathcal{B}_n = \mathcal{D} \cdot \text{Fix}(\mathbf{1}) \cdot \mathcal{D}_1 = \Phi(\mathcal{D} \times \text{Fix}(\mathbf{1}) \times \mathcal{D}_1)$. In particular, \mathcal{B}_n is a closed, pathwise connected subset of $U(n)$.

Proof. As we mentioned before, the equality $\mathcal{B}_n = \mathcal{D} \cdot \text{Fix}(\mathbf{1}) \cdot \mathcal{D}_1$ follows immediately from Theorem 4.1(a). Thus, by definition, $\mathcal{B}_n = \Phi(\mathcal{D} \times \text{Fix}(\mathbf{1}) \times \mathcal{D}_1)$. Since the subgroups \mathcal{D} , $\text{Fix}(\mathbf{1})$, \mathcal{D}_1 are compact and pathwise connected, \mathcal{B}_n , which is the continuous image of their cartesian product, has the same properties. \square

Moreover, the preimage $\Phi^{-1}(A)$ bijectively corresponds to $\text{Bi}(A)$.

Proposition 9.2. There is a continuous bijection between $\text{Bi}(A)$ and $\Phi^{-1}(A)$.

Proof. With the notation that D_u is a diagonal matrix with entries on the diagonal given by $u \in \mathbb{C}^n$, the bijection can be described as follows. The preimage $\Phi^{-1}(A)$ consists of all triplets $(D_1, S, D_2) \in \mathcal{D} \times \text{Fix}(\mathbf{1}) \times \mathcal{D}_1$ such that $A = D_1 S D_2$. In light of Proposition 3.1 this means that $D_2 = D_{\bar{v}}$ with $v \in \text{Bi}(A)$, $D_1 = D_{Av}$, and $S = D_{Av}^{-1} A D_{\bar{v}}^{-1} = D_{\overline{Av}} A D_v$. Therefore, the projection $(D_1, S, D_2) \rightarrow D_2$ and the map $D_u \rightarrow \bar{u}$ yield the continuous bijection from $\Phi^{-1}(A)$ onto $\text{Bi}(A)$, that is given by $(D_1, S, D_u) \rightarrow \bar{u}$. \square

Remark 9.3. $U(n)$ has (real) dimension n^2 , whereas $\text{Fix}(\mathbf{1}) \cong U(n-1)$ is of dimension $(n-1)^2$. \mathcal{D} has dimension n and \mathcal{D}_1 has dimension $n-1$, hence Φ is a mapping between two manifolds of (real) dimension n^2 . Clearly, Φ is smooth.

9.2 The structure of \mathcal{B}_n

In this subsection we show, that for every $n \in \mathbb{N}$ the set \mathcal{B}_n contains a nonempty open subset of $U(n)$. This is done by calculating the Jacobian of the map $\Phi : \mathcal{D} \times \text{Fix}(\mathbf{1}) \times \mathcal{D}_1 \rightarrow U(n)$ and proving that at a certain point it has a full rank. This allows to apply the inverse function theorem to draw the above conclusion.

In order to proceed with the calculations we provide some basic facts from the theory of Lie groups and establish the necessary notation.

We consider $U(n)$ and its subgroups as (real) submanifolds of the space $\mathfrak{gl}(n, \mathbb{C})$ of arbitrary matrices. Given a closed subgroup $H \subseteq GL(n, \mathbb{C})$ and $g \in H$, the tangent space $T_g H$ is the space of all tangent vectors of curves in H going through g , conveniently viewed as elements of the ambient space $\mathfrak{gl}(n, \mathbb{C})$ containing H . The tangent space $T_e H$ is a Lie-subalgebra of $\mathfrak{gl}(n, \mathbb{C})$, i.e. it is closed under the Lie bracket $[X, Y] = XY - YX$, and it is referred to as the Lie algebra \mathfrak{h} of H . Here, e is the neutral element, that is, the identity matrix that we shall denote by I . An alternative description of \mathfrak{h} is obtained via the matrix exponential, defined by

$$\exp(X) = \sum_{k=0}^{\infty} \frac{X^k}{k!}.$$

It is easy to verify that $\frac{d}{dt}(t \mapsto \exp(tX))|_{t=0} = X$, and \mathfrak{h} consists of all matrices X such that $\exp(tX) \in H$, for all $t \in \mathbb{R}$.

Since multiplication (on the left or on the right) with a group element g is a diffeomorphism on H , that is a matrix group, one obtains that

$$T_g H = g \cdot \mathfrak{h} = \{gX : X \in \mathfrak{h}\} = \mathfrak{h} \cdot g = \{Xg : X \in \mathfrak{h}\}.$$

We let $\mathfrak{u}, \mathfrak{d}, \mathfrak{d}_1, \mathfrak{f}$ denote the Lie algebras of $U(n), \mathcal{D}, \mathcal{D}_1, \text{Fix}(\mathbf{1})$, respectively. Then

$$\mathfrak{u} = \{X \in \mathfrak{gl}(n, \mathbb{C}) : X^* = -X\},$$

\mathfrak{d} consists of all diagonal matrices with purely imaginary entries, and $\mathfrak{d}_1 \subset \mathfrak{d}$ is the subspace of matrices with vanishing upper left corner. Differentiating the equality $\exp(tX)\mathbf{1} = \mathbf{1}$ at $t = 0$ yields the following description of \mathfrak{f} :

$$\mathfrak{f} = \{X \in \mathfrak{u} : X\mathbf{1} = 0\} ,$$

i.e. the elements of \mathfrak{f} are characterized by the fact that the sum over rows are zero. We also note the simple fact that $\mathfrak{d} \cap \mathfrak{f} = \{0\}$.

Finally, recall the definition of Jacobians. If $F : X \rightarrow Y$ is a smooth map between manifolds X and Y , the Jacobian of F at $x \in X$ is the linear map $dF(x) : T_x X \rightarrow T_{F(x)} Y$ defined as follows: For any $v \in T_x X$ pick a curve $\gamma : (-\epsilon, \epsilon) \rightarrow X$ with $\gamma(0) = x$, $\dot{\gamma}(0) = v$. Define the curve $\tilde{\gamma} = F \circ \gamma : (-\epsilon, \epsilon) \rightarrow Y$ (by definition $\tilde{\gamma}(0) = F(x)$). Then $dF(x)(v) = \dot{\tilde{\gamma}}(0)$.

To calculate the Jacobian of $\Phi : \mathcal{D} \times \text{Fix}(\mathbf{1}) \times \mathcal{D}_1 \rightarrow U(n)$ we shall use the following

Lemma 9.4. *Let H_1, H_2 be closed subgroups of $U(n)$ and $m : H_1 \times H_2 \rightarrow U(n)$, $m(g, h) = g \cdot h$. Then, for all $g, h \in U(n)$, the Jacobian of m at (g, h) is given by*

$$dm(g, h)(X, Y) = gY + Xh , \quad \forall X \in T_g H_1, Y \in T_h H_2 .$$

Proof. Let $\gamma_i : (-\epsilon, \epsilon) \rightarrow H_i$ denote smooth curves with

$$\gamma_1(0) = g, \dot{\gamma}_1(0) = X \text{ and } \gamma_2(0) = h, \dot{\gamma}_2(0) = Y .$$

By a standard reasoning, the product rule for scalar-valued functions easily extends to matrix-valued functions implying that

$$\frac{d(\gamma_1(t)\gamma_2(t))}{dt}(0) = \dot{\gamma}_1(0)\gamma_2(0) + \gamma_1(0)\dot{\gamma}_2(0) = gY + Xh .$$

□

Using this lemma and the chain rule, we obtain a rather transparent description of the Jacobian $d\Phi(D_1, S, D_2)$:

Lemma 9.5. *Let $(D_1, S, D_2) \in \mathcal{D} \times \text{Fix}(\mathbf{1}) \times \mathcal{D}_1$. Then*

$$d\Phi(D_1, S, D_2) : T_{D_1} \mathcal{D} \times T_S(\text{Fix}(\mathbf{1})) \times T_{D_2} \mathcal{D}_1 \rightarrow T_{D_1 S D_2} U(n)$$

acts via

$$d\Phi(D_1, S, D_2)(X, Y, Z) = D_1(SZ + YD_2) + XSD_2$$

Proof. Since we can factor

$$\Phi : (D_1, S, D_2) \mapsto (D_1, m(S, D_2)) \mapsto m(D_1, m(S, D_2)) ,$$

applying the previous lemma twice and using the chain rule yields

$$\begin{aligned} d\Phi(D_1, S, D_2)(X, Y, Z) &= [dm(D_1, SD_2) \circ (I, dm(S, D_2))](X, Y, Z) \\ &= dm(D_1, SD_2)(X, SZ + YD_2) = D_1(SZ + YD_2) + XSD_2 . \end{aligned}$$

□

Recall that we are particularly interested in the rank of $d\Phi$, that is, the real dimension of the image of $d\Phi$. The following lemma translates this to a more tractable problem in linear algebra:

Lemma 9.6. *Let $S \in \text{Fix}(\mathbf{1})$ be given, and $m \in \mathbb{N}$. Then the following are equivalent:*

- (a) *For all (any) $(D_1, D_2) \in \mathcal{D} \times \mathcal{D}_1$ the Jacobian $d\Phi(D_1, S, D_2)$ has rank m .*
- (b) *$d\Phi(I, S, I)$ has rank m .*

(c) *The linear map*

$$C_S : \mathfrak{d} \times \mathfrak{f} \times \mathfrak{d}_1 \rightarrow \mathfrak{u} , \quad (X, Y, Z) \mapsto X + Y + SZS^*$$

has rank m .

Proof. For the equivalence (a) \Leftrightarrow (b) we observe that $\Phi(CD_1, S, D_2C') = C\Phi(D_1, S, D_2)C'$ for all $C \in \mathcal{D}$, and $C' \in \mathcal{D}_1$. Thus, by the chain rule, $d\Phi(CD_1, S, D_2C') = Cd\Phi(D_1, S, D_2)C'$, what yields the equivalence.

To see that (b) \Leftrightarrow (c) we note, that by the previous lemma, $d\Phi(I, S, I)(X, Y', Z) = XS + Y' + SZ$, for all $X \in \mathfrak{d}, Y' \in T_S(\text{Fix}(\mathbf{1})), Z \in \mathfrak{d}_1$. Since S is invertible, the rank of $d\Phi(I, S, I)$ equals the rank of $R_{S^*} \circ d\Phi(I, S, I)$, where R_{S^*} denotes right multiplication with S^* . Clearly, $R_{S^*} \circ d\Phi(I, S, I)(X, Y', Z) = X + Y'S^* + SZS^*$ and this map has the same rank as the map C_S from (c), since $Y = Y'S^* \in \mathfrak{f}$ iff $Y' \in T_S(\text{Fix}(\mathbf{1}))$. \square

We next translate the condition from part (c) of the previous lemma to a simpler one. In the following lemma and its proof, the real and imaginary parts of complex vectors and matrices are computed componentwise. In particular, given a complex-valued matrix U , $\text{Im}(U)$ is obtained by taking the imaginary parts of the individual entries of U and the rank of $\text{Im}(U)$ is its rank as a mapping on \mathbb{R}^n . Also note that throughout the proof of the lemma, “linear” means “ \mathbb{R} -linear”; and matrices are identified with the linear map they induce.

Lemma 9.7. *Let $S \in \text{Fix}(\mathbf{1})$, then*

$$\text{rank}(d\Phi(I, S, I)) = (n - 1)^2 + n + \text{rank}(\text{Im}(S)) . \quad (13)$$

Proof. Let $C_S : \mathfrak{d} \times \mathfrak{f} \times \mathfrak{d}_1 \rightarrow \mathfrak{u}$ denote the linear map from Lemma 9.6. Let $\mathfrak{n} = \mathfrak{d} + \mathfrak{f} \subset \mathfrak{u}$. Then $\mathfrak{d} \cap \mathfrak{f} = \{0\}$ implies that the restriction of C_S to $\mathfrak{d} \times \mathfrak{f}$ is an isomorphism onto \mathfrak{n} . This allows for the first step towards (13) by considering the quotient map

$$\overline{C}_S : \mathfrak{d}_1 \rightarrow \mathfrak{u}/\mathfrak{n} , \quad Z \mapsto SZS^* + \mathfrak{n} ,$$

By Lemma 9.6 and a rank formula for the quotient map we obtain that

$$\text{rank}(d\Phi(I, S, I)) = \text{rank}(C_S) = \text{rank}(C|_{\mathfrak{d} \times \mathfrak{f}}) + \text{rank}(\overline{C}_S) = (n - 1)^2 + n + \text{rank}(\overline{C}_S) . \quad (14)$$

In order to prove that $\text{rank}(\overline{C}_S) = \text{rank}(\text{Im}(S))$, we need to free ourselves from the quotient space $\mathfrak{u}/\mathfrak{n}$. For this purpose, let us consider the map $T : \mathfrak{u} \rightarrow \mathbb{C}^n$, $T(X) = X\mathbf{1}$. We claim that

$$T(\mathfrak{u}) = V := \{x \in \mathbb{C}^n : \text{Re}\langle x, \mathbf{1} \rangle = 0\} .$$

Indeed, the kernel of T is precisely \mathfrak{f} , which has real codimension $2n - 1 = \dim_{\mathbb{R}}(V)$. Thus it suffices to prove that $T(\mathfrak{u}) \subset V$. This, however, follows from the fact that $X = -X^*$, for all $X \in \mathfrak{u}$, since

$$\text{Re}\langle T(X), \mathbf{1} \rangle = \text{Re}\langle X\mathbf{1}, \mathbf{1} \rangle = \text{Re}\langle \mathbf{1}, X^*\mathbf{1} \rangle = \text{Re}\langle -X\mathbf{1}, \mathbf{1} \rangle = -\text{Re}\langle T(X), \mathbf{1} \rangle .$$

We next consider the linear map $J : \mathfrak{u} \rightarrow \mathbb{R}^n$, $J(X) = \text{Re}(T(X))$. The kernel of J is then given by \mathfrak{n} , as can be seen by yet another dimension argument. The observation that $T(\mathfrak{u}) = V$ yields that

$$J(\mathfrak{u}) = \{\text{Re}(v) : v \in T(\mathfrak{u})\} = \{w \in \mathbb{R}^n : \langle w, \mathbf{1} \rangle = 0\} ,$$

so $J(\mathfrak{u})$ is a subspace of \mathbb{R}^n of dimension $n - 1$. Since the real codimension of \mathfrak{n} is also $n - 1$, it is enough to show that $\mathfrak{n} \subset \ker(J)$. For the latter, note that $J(X + Y) = J(X) = \text{Re}(x_1, \dots, x_n)$, for all $Y \in \mathfrak{f}$ and $X = \text{diag}(x_1, \dots, x_n) \in \mathfrak{d}$. Recall that $X \in \mathfrak{d}$ entails in addition $x_k \in i\mathbb{R}$, whence $J(X + Y) = 0$, establishing that $\ker(J) = \mathfrak{n}$.

This allows to conclude that J induces an *injective* linear map $\bar{J} : \mathfrak{u}/\mathfrak{n} \rightarrow \mathbb{R}^n$. Hence, if we define $Q = \bar{J} \circ \bar{C}_S$, then we obtain that $\text{rank}(\bar{C}_S) = \text{rank}(Q)$.

Clearly, $Q : \mathfrak{d}_1 \rightarrow \mathbb{R}^n$ and this map is much easier to treat than \bar{C}_S . Indeed, given any $Z \in \mathfrak{d}_1$, we employ $S^* \mathbf{1} = \mathbf{1}$ to compute that

$$Q(Z) = \text{Re}(SZS^* \mathbf{1}) = \text{Re}(SZ \mathbf{1}) = -\text{Im}(S)z ,$$

where $z = (0, z_2, \dots, z_n) \in \mathbb{R}^n$ is related to Z via $Z = \text{diag}(0, iz_2, \dots, iz_n)$. This shows that $\text{rank}(Q) = \text{rank}(\text{Im}(S)|_{W_0})$, where $W_0 \subset \mathbb{R}^n$ is the subspace of vectors with first entry equal to zero. Moreover, $W_0 + \mathbb{R} \cdot \mathbf{1} = \mathbb{R}^n$ and $\text{Im}(S)\mathbf{1} = 0$, since $S\mathbf{1} = \mathbf{1}$. Hence $\text{rank}(\text{Im}(S)|_{W_0}) = \text{rank}(\text{Im}(S))$.

Thus, we have established that $\text{rank}(\bar{C}_S) = \text{rank}(\text{Im}(S))$, so equation (13) follows from (14). \square

The above lemma leads to the fundamental fact, that for all $n \in \mathbb{N}$ the maximal rank of $d\Phi$ equals the dimension of $U(n)$.

Lemma 9.8. *For all $n \in \mathbb{N}$ there is an $S \in \text{Fix}(\mathbf{1}) \subset U(n)$ with $\text{rank}(d\Phi(I, S, I)) = n^2$.*

Proof. Let $W_{\mathbb{R}} \subset \mathbb{R}^n$ denote the orthogonal complement of $\mathbb{R} \cdot \mathbf{1}$ in \mathbb{R}^n , and $W_{\mathbb{C}} \subset \mathbb{C}^n$ denote the orthogonal complement of $\mathbb{C} \cdot \mathbf{1}$ in \mathbb{C}^n . In order to exhibit $S \in \text{Fix}(\mathbf{1})$ with $\text{rank}(d\Phi(I, S, I)) = n^2$ let us pick $S' \in \text{Fix}(\mathbf{1}) \cap O(n)$, where $O(n)$ stands for the orthogonal group. This entails $S'(W_{\mathbb{R}}) = W_{\mathbb{R}}$, so we can define a unitary mapping S on $W_{\mathbb{C}} \oplus \mathbb{C} \cdot \mathbf{1}$ by

$$S(v + \alpha \mathbf{1}) = iS'v + \alpha \mathbf{1} , \quad \alpha \in \mathbb{C}, v \in W_{\mathbb{C}} .$$

Then $S \in \text{Fix}(\mathbf{1})$, with $\text{Im}(S)|_{W_{\mathbb{R}}} = S'|_{W_{\mathbb{R}}}$. Since $S'(W_{\mathbb{R}}) = W_{\mathbb{R}}$, the restriction $S'|_{W_{\mathbb{R}}}$ has rank $n - 1$. Moreover, $W_{\mathbb{R}} \oplus \mathbb{R} \cdot \mathbf{1} = \mathbb{R}^n$ and $\text{Im}(S)\mathbf{1} = 0$, so

$$\text{rank}(\text{Im}(S)) = \text{rank}(\text{Im}(S)|_{W_{\mathbb{R}}}) = \text{rank}(S'|_{W_{\mathbb{R}}}) = n - 1 .$$

Thus, Lemma 9.7 implies that $\text{rank}(d\Phi(I, S, I)) = n^2$. \square

With the above lemma we can draw the mentioned conclusion regarding the structure of \mathcal{B}_n .

Theorem 9.9. *For every $n \in \mathbb{N}$ the set $\mathcal{B}_n \subset U(n)$ has a nonempty open interior.*

Proof. By Proposition 9.1 $\mathcal{B}_n = \Phi(\mathcal{D} \times \text{Fix}(\mathbf{1}) \times \mathcal{D}_1)$ and Φ is a map between groups of dimension n^2 . Lemma 9.8 guarantees an existence of a point in $\mathcal{D} \times \text{Fix}(\mathbf{1}) \times \mathcal{D}_1$, where the Jacobian of Φ has the full rank. Therefore, by the inverse function theorem, Φ is a diffeomorphism around this point. \square

Corollary 9.10. *$\mathcal{B}_n = U(n)$ if and only if $\mathcal{B}_n \cdot \mathcal{B}_n \subset \mathcal{B}_n$.*

Proof. Clearly, $A \in \mathcal{B}_n$ iff $A^{-1} \in \mathcal{B}_n$. Therefore, \mathcal{B}_n is a symmetric subset of $U(n)$ that, by the above theorem, has a nonempty open interior. If, in addition, it is closed under multiplication, then \mathcal{B}_n must be an open subgroup. Since $U(n)$ is connected, it follows that $\mathcal{B}_n = U(n)$. The converse is clear. \square

The results of this subsection can be compared with a theorem of De Vos and De Baerdemacker based on Hurwitz parametrization and stating that $(\mathcal{B}_n)^{n-1} = U(n)$.

9.3 The structure of $\text{Bi}(A)$

Regarding the structure of $\text{Bi}(A)$ it is crucial to recall Conjecture 1.1. In light of the hypothesis imposed by Björck and Saffari, the main issue is to establish the cardinality of $\text{Bi}(A)$. Therefore, there is a merit in proving the following.

Proposition 9.11. *For almost all $A \in U(n)$ the set $\text{Bi}(A)$ is finite.*

Proof. This follows from Proposition 9.2 and Sard's theorem. By Proposition 9.2 we can replace $\text{Bi}(A)$ by $\Phi^{-1}(A)$. Clearly, we can concentrate on the case $\Phi^{-1}(A) \neq \emptyset$. Recall that the regular points of a smooth map are those for which the rank of the Jacobian is full; any point that is not regular is called critical. A regular value is a value, such that all the points in the preimage are regular. If A is a regular value of Φ , then $\Phi^{-1}(A)$ must be a discrete subset of the compact space $\mathcal{D} \times \text{Fix}(\mathbf{1}) \times \mathcal{D}_1$, hence finite. Thus, if $\Phi^{-1}(A)$ is infinite, then A must be the image of a critical point of Φ . However, Sard's theorem states that the images of the critical points constitute a set of the Haar measure zero, what concludes the proof. \square

In order to achieve a deeper understanding of the set $\text{Bi}(A)$ for a given $A \in U(n)$, we consider the *phasing manifold* of A

$$\mathcal{M}_A = \mathcal{D}A\mathcal{D}_1$$

introduced in [49], and the stabilizer group $\mathcal{D}_A = \{(E_1, E_2) \in \mathcal{D} \times \mathcal{D}_1 : E_1 A E_2 = A\}$.

By Proposition 9.2 the next result establishes a bijection

$$\text{Bi}(A) \longleftrightarrow (\mathcal{M}_A \cap \text{Fix}(\mathbf{1})) \times \mathcal{D}_A ,$$

that can be explained in the following way. Intuitively, finding all biunimodular vectors for A amounts to finding all $S \in \text{Fix}(\mathbf{1})$ for which there exists a pair $(D_1, D_2) \in \mathcal{D} \times \mathcal{D}_1$ such that $A = D_1 S D_2$ (i.e. $S = D_1^{-1} A D_2^{-1} \in \mathcal{M}_A$) and, after that, finding other such pairs for S by considering the set $\{(D_1 E_1, D_2 E_2) : (E_1, E_2) \in \mathcal{D}_A\}$. We shall prove that this simple scheme yields all members of $\text{Bi}(A)$ in a one-to-one fashion.

Theorem 9.12. *There is a bijection $\Psi : (\mathcal{M}_A \cap \text{Fix}(\mathbf{1})) \times \mathcal{D}_A \rightarrow \Phi^{-1}(A)$.*

Proof. We can pick a map $\psi : \mathcal{M}_A \cap \text{Fix}(\mathbf{1}) \rightarrow \mathcal{D} \times \mathcal{D}_1$, $\psi(S) = (\psi_1(S), \psi_2(S))$, such that $\psi_1(S) S \psi_2(S) = A$. Indeed, by definition, for every $S \in \mathcal{M}_A \cap \text{Fix}(\mathbf{1})$ there is $(D_1, D_2) \in \mathcal{D} \times \mathcal{D}_1$, such that $S = D_1 A D_2$, thus we can pick one of such pairs and set $(\psi_1(S), \psi_2(S)) = (D_1^{-1}, D_2^{-1})$.

Then, the map $\Psi : (\mathcal{M}_A \cap \text{Fix}(\mathbf{1})) \times \mathcal{D}_A \rightarrow \Phi^{-1}(A)$ is given by

$$\Psi(S, (E_1, E_2)) = (E_1 \psi_1(S), S, E_2 \psi_2(S)) .$$

To see that the image of Ψ is contained in $\Phi^{-1}(A)$, it is enough to note that

$$\Phi(\Psi(S, (E_1, E_2))) = E_1 \psi_1(S) S \psi_2(S) E_2 = E_1 A E_2 = A .$$

The map is one-to-one, since $\Psi(S, (E_1, E_2)) = \Psi(S', (E'_1, E'_2))$ implies that $S = S'$ and this, in turn, implies that $E_i = E'_i$, for $i = 1, 2$. To check that the map is onto, we take an arbitrary element $(G_1, S, G_2) \in \Phi^{-1}(A)$ and easily verify that $\Psi(S, (E_1, E_2)) = (G_1, S, G_2)$ with $E_i = G_i (\psi_i(S))^{-1}$, for $i = 1, 2$. Since $G_1 (\psi_1(S))^{-1} A (\psi_2(S))^{-1} G_2 = G_1 S G_2 = A$, we get that $(E_1, E_2) \in \mathcal{D}_A$ and end the proof. \square

Remark 9.13. *Since in the above theorem it is hard to guarantee the continuity of ψ , we can not conclude that the bijection Ψ is continuous. We mention this, because otherwise, by Proposition 9.2 the set $\text{Bi}(A)$ would be homeomorphic to $(\mathcal{M}_A \cap \text{Fix}(\mathbf{1})) \times \mathcal{D}_A$.*

With Theorem 9.12, we can concentrate on the set $(\mathcal{M}_A \cap \text{Fix}(\mathbf{1})) \times \mathcal{D}_A$, in order to investigate the cardinality of $\text{Bi}(A)$. For that, we need a better understanding of the phasing manifold \mathcal{M}_A , for a given $A \in U(n)$. This can be obtained by defining the mapping

$$\Phi_A : \mathcal{D} \times \mathcal{D}_1 \rightarrow U(n) , \quad \Phi_A(D_1, D_2) = D_1 A D_2$$

and noting that $\mathcal{M}_A = \Phi_A(\mathcal{D} \times \mathcal{D}_1)$. This setup allows for making some useful observations.

Lemma 9.14. *For every $A \in U(n)$ the set \mathcal{M}_A is the orbit of A under the left action of $\mathcal{D} \times \mathcal{D}_1$ on $U(n)$ given by $((D_1, D_2), A) \mapsto D_1 A D_2$. In particular, \mathcal{M}_A is a closed submanifold of $U(n)$ with $\mathcal{M}_A \simeq (\mathcal{D} \times \mathcal{D}_1) / \mathcal{D}_A$, so $\dim(\mathcal{M}_A) + \dim(\mathcal{D}_A) = 2n - 1$.*

Proof. Note that the map $((D_1, D_2), A) \mapsto D_1 A D_2$ indeed defines an action of the product group, since the diagonal group is commutative; and clearly \mathcal{M}_A is the orbit of A . The remaining statements follow from this: Φ_A is just the quotient map with respect to this action, what implies that the differential of Φ_A has constant rank; and this in turn allows to define a manifold structure on \mathcal{M}_A . In addition, \mathcal{M}_A is compact, hence closed, and Φ_A induces a continuous bijection $(\mathcal{D} \times \mathcal{D}_1) / \mathcal{D}_A \rightarrow \mathcal{M}_A$ between compact Hausdorff spaces, which then has to be a homeomorphism. Therefore, $\dim(\mathcal{M}_A) + \dim(\mathcal{D}_A) = \dim(\mathcal{D} \times \mathcal{D}_1) = 2n - 1$. \square

Corollary 9.15. $\dim(\mathcal{M}_A) = 2n - 1 \iff \dim(\mathcal{D}_A) = 0 \iff \mathcal{D}_A$ is finite.

Proof. The first equivalence follows immediately from the dimension formula given in the above lemma. In the second equivalence one implication is obvious. For the other implication we note that, if $\dim(\mathcal{D}_A) = 0$ then \mathcal{D}_A must be a discrete subgroup of the compact group $\mathcal{D} \times \mathcal{D}_1$, so it must be finite. \square

At this stage we can provide the following explanation on the cardinality $|\text{Bi}(A)|$ of $\text{Bi}(A)$.

Obviously, for $n = 1$ we have $|\text{Bi}(A)| = 1$. When $n = 2$, then $|\text{Bi}(A)|$ equals to 2 or to the continuum \mathfrak{c} . For $n = 3$ we have only found examples where $|\text{Bi}(A)|$ equals to 4, 5, 6 or \mathfrak{c} . By Theorem 9.12, $|\text{Bi}(A)|$ is equal to the cardinality of the set $(\mathcal{M}_A \cap \text{Fix}(\mathbf{1})) \times \mathcal{D}_A$. Therefore, to see the general picture, we employ the above corollary together with Theorem 3.4 and get the following:

1. If $\dim(\mathcal{M}_A) < 2n - 1$ then $|\text{Bi}(A)| = \mathfrak{c}$.
2. If $\dim(\mathcal{M}_A) = 2n - 1$ then
 - (a) $|\text{Bi}(A)| \in \mathbb{N}$ or
 - (b) $\text{Bi}(A)$ is infinite but countable (no examples) or
 - (c) $\text{Bi}(A)$ is uncountable.

Remark 9.16. *Regarding the case $\dim(\mathcal{M}_A) < 2n - 1$, it is clear that for the identity matrix I (and any diagonal matrix) we have that $\mathcal{M}_I = \mathcal{D}$, so $\dim(\mathcal{M}_I) = n$. Moreover, there are examples of matrices $A \in U(n)$ with $\dim(\mathcal{M}_A)$ in the range from n to $2n - 1$.*

We would like to end this section by getting closer to understanding the classical Fourier case. As it turns out, for the Fourier matrix F_n the stabilizer \mathcal{D}_{F_n} is trivial.

Lemma 9.17. *For every $n \in \mathbb{N}$ we have that $\mathcal{D}_{F_n} = (I, I)$.*

Proof. Let $(E_1, E_2) \in \mathcal{D}_{F_n}$, i.e. $(E_1, E_2) \in \mathcal{D} \times \mathcal{D}_1$ and $E_1 F_n E_2 = F_n$. Then $E_2 = F_n^* E_1^* F_n$. This means that E_2 commutes with all translations (time shifts) and all modulations (frequency shifts). A result going back to Schwinger asserts that translations and modulations generate a basis for the space of all matrices $\mathfrak{gl}(n, \mathbb{C})$.⁴ Therefore, E_2 commutes with all matrices in this space, so $E_2 = \pm I$. Since $E_2 \in \mathcal{D}_1$, we get that $E_2 = I$, so $E_1 = I$ as well. \square

The above lemma together with Theorem 9.12 and Lemma 9.14 entail the following information on the set of all biunimodular vectors in the classical Fourier case.

Theorem 9.18. *For every $n \in \mathbb{N}$ there is a bijection between $\text{Bi}(F_n)$ and $\mathcal{M}_{F_n} \cap \text{Fix}(\mathbf{1})$, where \mathcal{M}_{F_n} is the phasing manifold of dimension $2n - 1$.*

⁴If T is a time shift by one, and M is a similar frequency shift, then $\{\frac{1}{\sqrt{n}} T^k M^l : k, l = 1, \dots, n\}$ form an orthonormal basis of $\mathfrak{gl}(n, \mathbb{C})$ (see [47]).

The above theorem indicates the resilience of Conjecture 1.1. Another approach towards this conjecture has been designed by Gabidulin. Unfortunately, even in the prime case, where some details are provided, he does not explain how to exclude that $\text{Bi}(F_n)$ is infinite but countable. Therefore, the only accessible confirmation of the conjecture in the prime case is [35].

10 Numerical Results

10.1 A simple algorithm and its properties

In the proof of Theorem 4.1(b) we have shown that $\|A\|_{\infty \rightarrow 1} \leq n$ for every $A \in U(n)$. As we pointed out in Remark 4.2, biunimodular vectors for A are precisely those, where the norm $\|A\|_{\infty \rightarrow 1} = n$ is attained. Thus, if v is a biunimodular vector of A , then we can think of it as of a point on \mathbb{T}^n , where the norm $\|Av\|_1$ is maximized.

In order to maximize the ℓ^1 -norm it is convenient to notice, that for every $v \in \mathbb{C}^n$ with $|v| \leq 1$ (entrywise) and $A \in U(n)$ we have that

$$\|Av\|_1 = \langle Av, \text{sign}(Av) \rangle = \langle v, A^*(\text{sign}(Av)) \rangle \leq \|A^*(\text{sign}(Av))\|_1, \quad (15)$$

where “sign” is the standard signum function defined on the support of $v \in \mathbb{C}^n$ by

$$\text{sign}(v) = \frac{v}{|v|},$$

so that $v = \text{sign}(v)|v|$. Since (15) holds for all v with $|v| \leq 1$, we can safely define $\text{sign}(v)$ as zero on the complement of the support of v .

Applying (15) twice yields

$$\|Av\|_1 \leq \|A^*(\text{sign}(Av))\|_1 \leq \|A(\text{sign}(A^*(\text{sign}(Av))))\|_1 := \|Av'\|_1, \quad (16)$$

with $v' = \text{sign}(A^*(\text{sign}(Av)))$. This leads to the following algorithm that with each step increases the ℓ^1 -norm of A on consecutive vectors, and therefore, allows to search for the biunimodular vectors of A .

1. **Initialization:** Take any vector $V_0 \in \mathbb{T}^n$.
2. **Step:** $V_{j+1} = \text{sign}(A^*(\text{sign}(AV_j)))$ for $j = 0, 1, \dots$

Clearly, (16) assures that

$$\|AV_j\|_1 \leq \|AV_{j+1}\|_1 \quad \text{for } j = 0, 1, \dots \quad (17)$$

giving a way to stop the algorithm after reaching J such that $\|AV_J\|_1 = n$. Of course, for numerical algorithms we can only expect this to hold within a certain, predefined precision. Since we know that $\|AV_j\|_1 \leq n$ for all $j \in \mathbb{N}$, we can set this precision to $\delta > 0$ and stop the algorithm after reaching a J such that

$$\|AV_J\|_1 > n - \delta. \quad (18)$$

In this way we rediscover a phase retrieval method that has a pretty long history. To make it short, following Jamming [37] we recall that as early as 1932, Pauli was asking whether the information on the moduli of a wave function and its Fourier transform allows to recover the phase of the wave function (i.e. Having $|\psi|$ and $|\mathcal{F}\psi|$ can we recover ψ ?). In practice, the phase retrieval problem is a serious obstacle for analysing complex valued signals, since only partial information is given on $|\psi|$ (see [18, 19] by Candès *et al.* or [4] and [29] for recent developments on this notorious problem). Nevertheless, under original Pauli constraints, a

method for recovering the phase of a signal has been provided in 1972 by Gerchberg and Saxton (see [32]). Gerchberg-Saxton algorithm has several variants, and the one that is relevant to us takes the following form. Let $|\psi| = g$ and $|\mathcal{F}\psi| = h$. In order to recover ψ define

$$P_{gh}f = g \operatorname{sign}_1(\mathcal{F}^*(h \operatorname{sign}_1(\mathcal{F}f))),$$

where

$$\operatorname{sign}_1(f) = \begin{cases} \frac{f}{|f|} & \text{on } \operatorname{supp}(f) \\ 1 & \text{off } \operatorname{supp}(f) \end{cases}$$

and starting with an f_0 such that $|f_0| = g$, run $f_j = P_{gh}^j(f_0)$ until it converges to a solution ψ' .⁵ This algorithm can be viewed as an alternating projection method for finding an intersection of two subsets of a Hilbert space, that was discovered by von Neumann in 1933 ([52]), in the case when the subsets are closed subspaces. This view is justified by writing P_{gh} as $P_G \circ P_H$, where $P_G f = g \operatorname{sign}_1(f)$ and $P_H f = \mathcal{F}^*(h \operatorname{sign}_1(\mathcal{F}f))$ are projections on certain subsets of a Hilbert space.

The method of alternating projections is a topic by itself (see [26]), that is well covered in the case of convex sets ([5]) and compact sets with a non-empty intersection ([21]). In our setting we are looking for an intersection of two compact non-convex sets, namely \mathbb{T}^n and $A^*(\mathbb{T}^n)$, with a guarantee that $\mathbb{T}^n \cap A^*(\mathbb{T}^n) \neq \emptyset$ provided by Theorem 3.4.

Clearly, $\operatorname{sign}_1 : \mathbb{C}^n \rightarrow \mathbb{T}^n$ is a projection on the torus (in the sense that $\|v - \operatorname{sign}_1(v)\|_2 = \operatorname{dist}(v, \mathbb{T}^n)$), and $A^* \circ \operatorname{sign}_1 \circ A$ is a projection on $A^*(\mathbb{T}^n)$. Thus, a successive application of $P'_A(v) = \operatorname{sign}_1(A^*(\operatorname{sign}_1(Av)))$ yields the standard alternating projection method.

Although we use

$$P_A(v) = \operatorname{sign}(A^*(\operatorname{sign}(Av))), \quad v \in \mathbb{C}^n, A \in U(n)$$

instead of P'_A , we shall quickly confine our search to the range where both these operators agree. Thus, we shall refer to this method as “alternating projection algorithm” anyway.

After providing this backdrop, we can take on understanding the workings of the algorithm. Recall that we start with an arbitrary vector $V_0 \in \mathbb{T}^n$ and successively apply P_A , by setting $V_j = P_A^j V_0$, until we reach a J such that (18) holds with a certain precision $\delta > 0$.

The price for the simplicity of this algorithm is its randomness, that has to be properly interpreted.⁶

Since $v \in \mathbb{T}^n$ is biunimodular for A iff $\|Av\|_1 = n$, we would be satisfied with finding V_J such that δ in (18) is close to zero. However, there is no guarantee that for a given starting vector V_0 we will find $J \in \mathbb{N}$ so that δ is small enough. This is already apparent in the case $A = F_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ with $V_0 = (1, 1)$. Indeed, here $V_j = V_0$ for all $j \in \mathbb{N}$, so $\|AV_j\|_1 = \sqrt{2} \ll 2$. Therefore, in general, the algorithm has to be applied to multiple random starting vectors in \mathbb{T}^n .

Another aspect of the randomness is due to the discontinuity of the signum function. Clearly, neither P_A nor P'_A is continuous. In theory, the vector $\mathbf{1} = (1, 1, \dots, 1) \in \mathbb{C}^n$ is a fix point of both P_A and P'_A , when $A = F_n$. In practice, both algorithms may converge to more stable solutions when applied to the starting vector $\mathbf{1}$ in the Fourier case. Of course, similar problems may occur in the general case as well. In order to avoid the discontinuity, we observe that for every $A \in U(n)$ and $v \in \mathbb{T}^n$ such that $\|Av\|_1 > n - \delta$ we have the following

$$\|\mathbf{1} - Av\|_2^2 = n - 2\|Av\|_1 + \|Av\|_2^2 = 2(n - \|Av\|_1) < 2\delta,$$

⁵Unfortunately, ψ' is not unique (it depends on the choice of f_0), so it is only a candidate for ψ (see Subsection 10.3).

⁶Essentially, one has to run the algorithm with multiple starting vectors in \mathbb{T}^n to get satisfactory results (see Subsection 10.2).

so $|Av| \geq \frac{1}{2}$ for $\delta \leq \frac{1}{8}$. Moreover, for such δ we get

$$\|A^*(\text{sign}(Av)) - v\|_2^2 = \|\text{sign}(Av) - Av\|_2^2 = \|\mathbf{1} - |Av|\|_2^2 < 2\delta,$$

so $|A^*(\text{sign}(Av))| \geq \frac{1}{2}$ as well. This allows to draw the following conclusions.

If the stopping condition (18) is satisfied, then $\|\mathbf{1} - |AV_J|\|_2 < \sqrt{2\delta}$. If the initial condition

$$\|AV_0\|_1 > n - \frac{1}{8} \quad (19)$$

is satisfied, then for all $j \in \mathbb{N} \cup \{0\}$ we have that

- $V_j := P_A^j V_0 = (P'_A)^j V_0$,
- $V_j \in \mathbb{T}^n$, $|AV_j| \geq \frac{1}{2}$ and $|A^*(\text{sign}(AV_j))| \geq \frac{1}{2}$,

due to an easy induction argument. Moreover, assuming (19), it can be proved that

- $\|AV_{j+1}\|_1 = \|AV_j\|_1$ iff $V_{j+1} = V_j$,
- $\lim_{j \rightarrow \infty} \|V_{j+1} - V_j\|_\infty = 0$.

Where the former follows from (15) and (16), while the proof of the latter is a bit lengthy, so we include it in Appendix B containing a detailed study of the algorithm.

Since the sequence $(\|AV_j\|_1)_{j \in \mathbb{N}}$ is monotonic and bounded, it converges to a limit $L \leq n$. In Appendix B we show that under the initial condition (19) the cluster points of $(V_j)_{j \in \mathbb{N}}$ belong to the set S_A of fix points of P_A . This allows to assure the convergence of V_j , in the case when S_A is finite. Since biunimodular vectors of A belong to S_A , we know that for some A the set S_A is uncountable. Thus, it is possible, that in some cases V_j does not converge.

This brings us to the main point of the analysis of the algorithm. If the stopping condition (18) holds with $\delta \leq \frac{1}{8}$, then the initial condition (19) holds with V_0 replaced by V_J . Thus, the stopping condition (18), with δ numerically near to zero, gives V_J that is close to a fix point of P_A . If $L := \lim_{j \rightarrow \infty} \|AV_j\|_1 = n$, then V_J is close to a biunimodular vector of A , however, it is not clear how close. If $L < n$, then V_J is close (in a similar fashion) to a fix point of P_A , that may be far away from biunimodular vectors. Moreover, it is impossible to establish numerically that $L = n$. Hence, we need to settle for δ -near biunimodular vectors given as

$$\text{Bi}_\delta(A) = \{v \in \mathbb{T}^n : \|Av\|_1 > n - \delta\}$$

and stress again, that some of these vectors can be far away from biunimodular vectors, even if δ is nearly zero.

In short, if the algorithm returns vectors that are “biunimodular” in practice, there is no guarantee that they are close to the theoretical biunimodular vectors.

Despite this uncertainty, it turns out, that finding near biunimodular vectors for every unitary matrix is sufficient to conclude, that all such matrices have biunimodular vectors. In the following proposition we prove even more.

Proposition 10.1. *Let $\alpha < 1$. If for every $n \in \mathbb{N}$ and for every $A \in U(n)$ there is $v \in \mathbb{T}^n$ such that*

$$\|Av\|_1 \geq n - n^\alpha, \quad (20)$$

then every unitary matrix has a biunimodular vector.

Proof. This follows from considering diagonal block matrices. If $B \in U(m)$ does not have biunimodular vectors, then $\|B\|_{\infty \rightarrow 1} = m - \epsilon$ with some $\epsilon > 0$. Therefore, for every $N \in \mathbb{N}$, the block matrix A_N with N copies of B on the diagonal

$$A_N := \begin{bmatrix} \boxed{B} & & & \\ & \boxed{B} & & \\ & & \ddots & \\ & & & \boxed{B} \end{bmatrix}$$

belonging to $U(n)$ with $n = Nm$, has the norm $\|A_N\|_{\infty \rightarrow 1} = N(m - \epsilon)$. Thus, if (20) holds for A_N , then we get that

$$n - n^\alpha \leq \|A_N v\|_1 \leq n - n \frac{\epsilon}{m},$$

leading to a contradiction $\frac{\epsilon}{m} \leq n^{\alpha-1}$, since $n^{\alpha-1} \rightarrow 0$ as $N \rightarrow \infty$. \square

In the next subsection we check the performance of the alternating projection algorithm for unitary matrices up to dimension 100. The final subsection contains results of the application of this algorithm to the Fourier case.

10.2 Effectiveness of the algorithm

In order to measure the performance of the alternating projection algorithm we recall, that for $\delta > 0$ and $A \in U(n)$ we have defined the set

$$\text{Bi}_\delta(A) = \{v \in \mathbb{T}^n : \|Av\|_1 > n - \delta\}$$

of δ -near biunimodular vectors of A . For a given unitary matrix A and a prescribed parameter δ the algorithm is supposed to return a member of $\text{Bi}_\delta(A)$. The effectiveness of the algorithm can be measured by considering the set $\mathcal{B}_{n,\delta}$, that is, the set of these matrices in $U(n)$, for which the algorithm returns the desired outcome.

The aim of this subsection is to provide numerical evidence that the Haar measure of $\mathcal{B}_{n,\delta}$ (that we denote by $\mu(\mathcal{B}_{n,\delta})$) is very close to one. For this purpose we proceeded as follows: For each dimension under consideration, we drew a fixed number K of random unitary matrices with Haar measure used as underlying probability measure. To achieve this, we implemented the method described in [41]. We then ran the alternating projection algorithm on the matrix with randomly chosen starting vectors, in order to produce near biunimodular vectors. The search was terminated either if one such vector was found, or until a maximal number of starting points was exceeded. The parameters used in this procedure were as follows:

- $\delta = 10^{-10}$.
- Dimensions: $n = 3, 5, 10, 25, 50, 75, 100$.
- Number of matrices: $K = 10^4$;
- Maximal number of starting points: $M = 10^3$;
- Maximal number of iterations: $L = 10^4$.

We implemented the described algorithms in MATLAB, and ran them on a stand-alone personal computer⁷.

The results of our numerical experiment are documented in Table 1. Two facts seem particularly striking to us: First of all, the algorithm found a δ -near biunimodular vector *for each of the 10^4 random matrices in each dimension considered*. This translates to an estimate of $\mu(\mathcal{B}_{n,\delta})$, which holds at least with very high likelihood: Our numerical experiment amounts to performing a Bernoulli experiment based on repeated independent samples of a Haar-distributed random matrix A in $U(n)$, and a positive outcome of the experiment (a near biunimodular vector being found) implies $A \in \mathcal{B}_{n,\delta}$. Thus the probability of a positive outcome for a single event is given by $p \leq \mu(\mathcal{B}_{n,\delta})$. Assuming that $\mu(\mathcal{B}_{n,\delta}) \leq 1 - 10^{-3} = 0.999$, the probability of obtaining a positive result 10^4 times in a row will thus be $\leq 0.999^{10^4} \approx 4.5173 \cdot 10^{-5}$. In other words, our experiments provide very convincing evidence that $\mu(\mathcal{B}_{n,\delta}) > 0.999$.

Another striking phenomenon is illustrated by the 3rd and 4th column of Table 1, highlighting the effectiveness of the search algorithm. For small to medium dimensions and in the

⁷The CPU of the machine was a 6 core AMD FX 6100 processor with 8 MB level 1 cache, running at 3.3 GHz, together with 8 GB RAM. The operating system was SUSE linux 12.2 for 64-bit PCs.

Dimension	Matrices in $\mathcal{B}_{n,\delta}$	starting points (average)	starting points (maximal)	total runtime (rounded)
3	10^4	1.0663	5	1 min 38 sec
5	10^4	1.1719	7	4 min 20 sec
10	10^4	1.3472	7	9 min 59 sec
25	10^4	1.6521	10	28 min 51 sec
50	10^4	2.4106	17	1 h 34 min
75	10^4	4.3361	34	5 h 6 min
100	10^4	9.4730	89	16 h 40 min

Table 1: Results of the numerical experiment

average case, the algorithm needs only very few starting points to find a near biunimodular vector, but even the maximal number of such points stays well away from the maximal number of 10^3 that was allowed. As the dimension increases, several effects conspire to increase the algorithm complexity: The rate of convergence in the alternating projection algorithm slows down, as witnessed by the increasing percentage of cases where the maximal number of iterations is reached before the $(n-\delta)$ -threshold is passed (not shown in the table). Also, one may expect that the chances of randomly picking starting points for which the alternating projection algorithm converges sufficiently quickly also diminish with increasing dimension. Both effects increase the number of starting points needed in the search. In addition, the costs of applying the matrix-by-vector multiplication also can be expected to contribute to a nonlinear increase of the computational load. It seems that the overall result is an exponential increase of runtime: A log-linear fit for the runtimes for $n \geq 10$ revealed a behaviour like $O(e^{0.05n})$.

10.3 Biunimodular vectors for Fourier matrices

The search for the biunimodular vectors for F_n via the alternating projection algorithm is the simplest realization of the phase retrieval process under trivial Pauli constraints $|\psi| \equiv |\mathcal{F}\psi| \equiv 1$ in the discrete Fourier case $\mathcal{F} = F_n$, $\psi \in \mathbb{C}^n$.

When looking for elements of $\text{Bi}(F_n)$ for a Fourier matrix F_n , it is advantageous to take into account various operations that preserve this set:

- Circular shifts by $k = 0, 1, \dots, n-1$. I.e., if $(u_0, \dots, u_{n-1}) \in \text{Bi}(F_n)$, then the vector $(u_k, u_{k+1}, \dots, u_{n-1}, u_0, \dots, u_{k-1})$ is biunimodular.
- Modulation by $k = 0, 1, \dots, n-1$: If $(u_0, \dots, u_{n-1}) \in \text{Bi}(F_n)$, then the vector $(u_0, u_1 \exp(2\pi i k/n), \dots, u_{n-1} \exp(2\pi i k(n-1)/n))$ is biunimodular.
- Dilation by $k = 0, 1, \dots, n-1$ coprime with n : If $(u_0, \dots, u_{n-1}) \in \text{Bi}(F_n)$, then (y_0, \dots, y_{n-1}) with $y_j = u_{jk \bmod n}$ is biunimodular.
- Conjugation: If $(u_0, \dots, u_{n-1}) \in \text{Bi}(F_n)$, then its conjugate $(\bar{u}_0, \dots, \bar{u}_{n-1}) \in \text{Bi}(F_n)$.
- Fourier transform: If $u \in \text{Bi}(F_n)$, then $F_n u$ is biunimodular as well.

These operations induce the action of a finite group G_n of size $4n^2\varphi(n)$ on $\text{Bi}(F_n)$, where $\varphi(n)$ is Euler's totient function.

We employed the alternating projection method to produce a list of near biunimodular vectors $v \in \text{Bi}_\delta(F_n)$, for $\delta = 10^{-7}$. More precisely, we computed a list of orbit representatives of such vectors, by repeatedly running the alternating projection algorithm with random starting points. For all dimensions, we used 10^4 starting vectors, and at most 30 000 iterations before starting with a new random vector. Whenever the algorithm terminated in a δ -near

biunimodular vector, the result was appended to the list, provided its ℓ^2 -distance to all orbits already on the list exceeded the threshold $\tau = 10^{-5}$.

There is a certain degree of arbitrariness in our choices of parameters. Regarding the choice of τ and δ , recall that we currently have no means of predicting how close a δ -near biunimodular vector is to an actual biunimodular vector (if at all). Also, an a priori choice of the threshold τ would have to be based on the knowledge of the local maxima of the mapping $v \mapsto \|Av\|_1$ on the torus. The above choice of τ was motivated by the observation that the orbits of known biunimodular vectors in dimensions up to 13 had a minimal ℓ^2 -distance $\geq 10^{-2}$ and 10^{-5} is safely below this value.

The procedure to compute near biunimodular vectors was applied to all square-free numbers between 2 and 15. In the following presentation of numerical results, we say that an orbit found by our algorithm is close to one from the literature, if the minimal distance (measured in $\|\cdot\|_2$) between them is $< 10^{-5}$. We observed that each time an orbit found by alternating projections was close to an orbit from the literature, the orbit cardinalities matched as well.

- $n = 2$: The algorithm precisely found the one orbit consisting of the two vectors $(1, \pm i)$.
- $n = 3$: The algorithm found one orbit of length 6, which was close to the orbit of the gaussian vector $(1, \omega^2, 1)$, where $\omega = \exp(2\pi i/3)$.
- $n = 5$: The algorithm found two orbits, each of length 10. Each orbit was close to one of the orbits represented by the gaussian vectors $(1, \omega, \omega^4, \omega^4, \omega)$ and $(1, \omega^2, \omega^3, \omega^3, \omega^2)$, where $\omega = \exp(2\pi i/5)$.
- $n = 6$: The algorithm found two orbits, one of length 12 and one of length 36. The orbit of length 12 was close to the gaussian vector, the orbit of length 36 was close to the vector described in [34, formula (3.20)].
- $n = 7$: The algorithm found three orbits, with lengths 42, 196 and 294, yielding 532 solutions in total. The orbit of length 42 is close to the gaussian solution, whereas the orbit of length 196 is close to the Björck sequence $(1, 1, 1, e^{i\theta}, 1, e^{i\theta}, e^{i\theta})$ mentioned in the introduction. The orbit of length 294 was close to the solution given in [34, formula (3.24)].
- $n = 10$: Here we obtained 10 orbits, with orbit lengths 20 (2 orbits), 200 (3 orbits), 400 (4 orbits), and 800 (1 orbit), resulting in a total of 3040 solutions. For $n = 10$, the literature does not provide a complete list of solutions.
- $n = 11$: Here 12 orbits were found, with lengths 110 (1), 484 (1), 1210 (7), 2420 (2) and 4840 (1), resulting in a total number of 18744 vectors. Among these were the gaussians, all contained in the orbit of length 110. For $n = 11$, the literature does not provide a complete list of solutions.
- $n = 13$: The algorithm found 20 orbits, with lengths 78 (2), 338 (2), 1014 (2), 1352 (2), 2028 (7), and 4056 (5), yielding 40040 solutions in total. Gabidulin and Shorin [30] exhibited 25 orbits for $n = 13$, with 53222 solutions overall. Each of the orbits found via alternating projections was close to precisely one orbit representative from the list presented by Gabidulin and Shorin. The following orbits given in [30] were not found by the algorithm: An orbit with 1014 elements, corresponding to the case $e = 6$ in [30, Subsection 7.4], two orbits with 2028 solutions, corresponding to lines one and seven in the table in [30, Subsection 7.4], and the first two orbits listed for the case $e = 12$, each having 4056 elements.
- $n = 14$: The algorithm found 39 orbits, with lengths 84 (1), 196 (2), 392 (1), 588 (3), 784 (2), 1176 (12), 2352 (13), 4704 (5), resulting in a total of 72408 vectors. Among these were the gaussians, all contained in the orbit of length 84. For $n = 14$, the literature does not provide a complete list of solutions.

- $n = 15$: The algorithm produced 46 orbits, with lengths 900 (2), 1800 (21), 3600 (20), 7200 (3), resulting in a total of 133200 vectors. The gaussian vectors are contained in two orbits of length 60, which were not found by the algorithm. For $n = 15$, the literature does not provide a complete list of solutions.

Appendix A

As we have already explained, Theorem 8.1 allows for an easy construction of all unitary matrices in the dyadic case $U(2^n)$. Recall, that every such matrix can be obtained from four matrices in $U(2^{n-1})$. For $n = 1$ the procedure yields $U(2)$ via (10). Here, we show how the procedure works in the case $n = 2$, to get a closed formula for $U(4)$.

For a collection of 16 unimodular parameters $a_j, b_j, c_j, z_j \in \mathbb{T}$ with $j = 0, 1, 2, 3$ we define the corresponding four matrices in $U(2)$ via (10):

$$\begin{aligned} A &= \frac{1}{2} \begin{bmatrix} a_1(1+a_0) & a_1a_3(1-a_0) \\ a_2(1-a_0) & a_2a_3(1+a_0) \end{bmatrix} & B &= \frac{1}{2} \begin{bmatrix} b_1(1+b_0) & b_1b_3(1-b_0) \\ b_2(1-b_0) & b_2b_3(1+b_0) \end{bmatrix} \\ C &= \frac{1}{2} \begin{bmatrix} c_1(1+c_0) & c_1c_3(1-c_0) \\ c_2(1-c_0) & c_2c_3(1+c_0) \end{bmatrix} & Z &= \frac{1}{2} \begin{bmatrix} z_1(1+z_0) & z_1z_3(1-z_0) \\ z_2(1-z_0) & z_2z_3(1+z_0) \end{bmatrix}. \end{aligned} \quad (21)$$

Theorem 8.1 asserts that every unitary matrix $U \in U(4)$ with entries $(U)_{k,l} = u_{k,l}$, where $k, l = 1, 2, 3, 4$, can be obtained as

$$U = \frac{1}{2} \begin{bmatrix} A(I+Z) & A(I-Z)C \\ B(I-Z) & B(I+Z)C \end{bmatrix}.$$

This gives the following description of $U(4)$:

$$\begin{aligned} u_{11} &= \frac{1}{2}(\frac{1}{4}a_1a_3(1-a_0)z_2(1-z_0) + \frac{1}{2}a_1(1+a_0)(1+\frac{1}{2}z_1(1+z_0))) \\ u_{21} &= \frac{1}{2}(\frac{1}{4}a_2a_3(1+a_0)z_2(1-z_0) + \frac{1}{2}a_2(1-a_0)(1+\frac{1}{2}z_1(1+z_0))) \\ u_{31} &= \frac{1}{2}(-\frac{1}{4}b_1b_3(1-b_0)z_2(1-z_0) + \frac{1}{2}b_1(1+b_0)(1-\frac{1}{2}z_1(1+z_0))) \\ u_{41} &= \frac{1}{2}(-\frac{1}{4}b_2b_3(1+b_0)z_2(1-z_0) + \frac{1}{2}b_2(1-b_0)(1-\frac{1}{2}z_1(1+z_0))) \\ \\ u_{12} &= \frac{1}{2}(\frac{1}{4}a_1(1+a_0)z_1z_3(1-z_0) + \frac{1}{2}a_1a_3(1-a_0)(1+\frac{1}{2}z_2z_3(1+z_0))) \\ u_{22} &= \frac{1}{2}(\frac{1}{4}a_2(1-a_0)z_1z_3(1-z_0) + \frac{1}{2}a_2a_3(1+a_0)(1+\frac{1}{2}z_2z_3(1+z_0))) \\ u_{32} &= \frac{1}{2}(-\frac{1}{4}b_1(1+b_0)z_1z_3(1-z_0) + \frac{1}{2}b_1b_3(1-b_0)(1-\frac{1}{2}z_2z_3(1+z_0))) \\ u_{42} &= \frac{1}{2}(-\frac{1}{4}b_2(1-b_0)z_1z_3(1-z_0) + \frac{1}{2}b_2b_3(1+b_0)(1-\frac{1}{2}z_2z_3(1+z_0))) \\ \\ u_{13} &= \frac{1}{2}(\frac{1}{2}c_1(1+c_0)(-\frac{1}{4}a_1a_3(1-a_0)z_2(1-z_0) + \frac{1}{2}a_1(1+a_0)(1-\frac{1}{2}z_1(1+z_0))) + \\ &\quad \frac{1}{2}c_2(1-c_0)(-\frac{1}{4}a_1(1+a_0)z_1z_3(1-z_0) + \frac{1}{2}a_1a_3(1-a_0)(1-\frac{1}{2}z_2z_3(1+z_0)))) \\ u_{23} &= \frac{1}{2}(\frac{1}{2}c_1(1+c_0)(-\frac{1}{4}a_2a_3(1+a_0)z_2(1-z_0) + \frac{1}{2}a_2(1-a_0)(1-\frac{1}{2}z_1(1+z_0))) + \\ &\quad \frac{1}{2}c_2(1-c_0)(-\frac{1}{4}a_2(1-a_0)z_1z_3(1-z_0) + \frac{1}{2}a_2a_3(1+a_0)(1-\frac{1}{2}z_2z_3(1+z_0)))) \\ u_{33} &= \frac{1}{2}(\frac{1}{2}c_1(1+c_0)(\frac{1}{4}b_1b_3(1-b_0)z_2(1-z_0) + \frac{1}{2}b_1(1+b_0)(1+\frac{1}{2}z_1(1+z_0))) + \\ &\quad \frac{1}{2}c_2(1-c_0)(\frac{1}{4}b_1(1+b_0)z_1z_3(1-z_0) + \frac{1}{2}b_1b_3(1-b_0)(1+\frac{1}{2}z_2z_3(1+z_0)))) \\ u_{43} &= \frac{1}{2}(\frac{1}{2}c_1(1+c_0)(\frac{1}{4}b_2b_3(1+b_0)z_2(1-z_0) + \frac{1}{2}b_2(1-b_0)(1+\frac{1}{2}z_1(1+z_0))) + \end{aligned}$$

$$\begin{aligned}
& \frac{1}{2}c_2(1-c_0)(\frac{1}{4}b_2(1-b_0)z_1z_3(1-z_0) + \frac{1}{2}b_2b_3(1+b_0)(1+\frac{1}{2}z_2z_3(1+z_0))) \\
u_{14} = & \frac{1}{2}(\frac{1}{2}c_1c_3(1-c_0)(-\frac{1}{4}a_1a_3(1-a_0)z_2(1-z_0) + \frac{1}{2}a_1(1+a_0)(1-\frac{1}{2}z_1(1+z_0))) + \\
& \frac{1}{2}c_2c_3(1+c_0)(-\frac{1}{4}a_1(1+a_0)z_1z_3(1-z_0) + \frac{1}{2}a_1a_3(1-a_0)(1-\frac{1}{2}z_2z_3(1+z_0))) \\
u_{24} = & \frac{1}{2}(\frac{1}{2}c_1c_3(1-c_0)(-\frac{1}{4}a_2a_3(1+a_0)z_2(1-z_0) + \frac{1}{2}a_2(1-a_0)(1-\frac{1}{2}z_1(1+z_0))) + \\
& \frac{1}{2}c_2c_3(1+c_0)(-\frac{1}{4}a_2(1-a_0)z_1z_3(1-z_0) + \frac{1}{2}a_2a_3(1+a_0)(1-\frac{1}{2}z_2z_3(1+z_0))) \\
u_{34} = & \frac{1}{2}(\frac{1}{2}c_1c_3(1-c_0)(\frac{1}{4}b_1b_3(1-b_0)z_2(1-z_0) + \frac{1}{2}b_1(1+b_0)(1+\frac{1}{2}z_1(1+z_0))) + \\
& \frac{1}{2}c_2c_3(1+c_0)(\frac{1}{4}b_1(1+b_0)z_1z_3(1-z_0) + \frac{1}{2}b_1b_3(1-b_0)(1+\frac{1}{2}z_2z_3(1+z_0))) \\
u_{44} = & \frac{1}{2}(\frac{1}{2}c_1c_3(1-c_0)(\frac{1}{4}b_2b_3(1+b_0)z_2(1-z_0) + \frac{1}{2}b_2(1-b_0)(1+\frac{1}{2}z_1(1+z_0))) + \\
& \frac{1}{2}c_2c_3(1+c_0)(\frac{1}{4}b_2(1-b_0)z_1z_3(1-z_0) + \frac{1}{2}b_2b_3(1+b_0)(1+\frac{1}{2}z_2z_3(1+z_0)))
\end{aligned}$$

with 16 parameters $a_j, b_j, c_j, z_j \in \mathbb{T}$, where $j = 0, 1, 2, 3$.

By setting $u_{11} = 1$ in the above formula for $U(4)$ we will find a description of $U(3)$, that is used in Theorem 6.3 to prove the existence of a biunimodular vector for every matrix in $U(3)$. This shall be executed as a series of observations.

First, we set $u_{11} = 1$ in the above formula for $U(4)$.

Observation A.1. $u_{11} := \frac{1}{2}(\frac{1}{4}a_1a_3(1-a_0)z_2(1-z_0) + \frac{1}{2}a_1(1+a_0)(1+\frac{1}{2}z_1(1+z_0))) = 1$ iff $a_0 = a_1 = z_0 = z_1 = 1$.

Proof. Clearly, $u_{11} = \frac{1}{2}\langle R, e + \overline{K} \rangle$, where $e = (1, 0)$, $R = \frac{1}{2}(a_1(1+a_0), a_1a_3(1-a_0))$ denotes the first row of A from (21) and $K = \frac{1}{2}(z_1(1+z_0), z_2(1-z_0))$ denotes the first column of Z from therein. Thus, $\|R\|_2 = \|K\|_2 = 1$.

Since u_{11} is an entry of a unitary matrix, we know that $|u_{11}| \leq 1$. This inequality can be proved directly in the following way

$$|u_{11}| = \frac{1}{2} |\langle R, e + \overline{K} \rangle| \leq \frac{1}{2} (|\langle R, e \rangle| + |\langle R, \overline{K} \rangle|) \leq \frac{1}{2} (\|R\|\|e\| + \|R\|\|K\|) = 1.$$

Therefore, $|u_{11}| = 1$ means that $|\langle R, e \rangle| = \|R\|\|e\|$, $|\langle R, \overline{K} \rangle| = \|R\|\|K\|$ (so $R = \lambda e$, $K = \mu e$ with $\lambda, \mu \in \mathbb{T}$) and $|\langle R, e + \overline{K} \rangle| = |\langle R, e \rangle| + |\langle R, \overline{K} \rangle|$ (so $\mu = 1$). Finally, $u_{11} = \frac{1}{2}\langle R, e + \overline{K} \rangle = 1$ gives $\lambda = 1$. Hence, $u_{11} = 1$ iff $R = K = e$, that is, $a_0 = a_1 = z_0 = z_1 = 1$. \square

Then, we set $a_0 = a_1 = z_0 = z_1 = 1$ in the formula for $U(4)$, to get a corresponding formula for $U(3)$ given by the simplified entries $u_{k,l}$ with $k, l = 2, 3, 4$. By pulling out some factors from these entries we obtain the following matrix: $D_1 U_{(a,b,c,z)} D_2$, where D_1 is the diagonal matrix $D_1 = \text{diag}(a_2a_3, b_1b_3, b_2b_3)$, $D_2 = \text{diag}(1, c_2, c_3)$ and

$$U_{(a,b,c,z)} = \begin{bmatrix} \frac{(1+a)}{2} & \frac{(1-a)(1-c)}{4} & \frac{(1-a)(1+c)}{4} \\ \frac{(1-a)(1-b)}{4} & z\frac{(1+b)(1+c)}{4} + \frac{(1+a)(1-b)(1-c)}{8} & z\frac{(1+b)(1-c)}{4} + \frac{(1+a)(1-b)(1+c)}{8} \\ \frac{(1-a)(1+b)}{4} & z\frac{(1-b)(1+c)}{4} + \frac{(1+a)(1+b)(1-c)}{8} & z\frac{(1-b)(1-c)}{4} + \frac{(1+a)(1+b)(1+c)}{8} \end{bmatrix},$$

with $a = z_2z_3$, $b = b_4$, $c = c_4$ and $z = \overline{c_1c_2b_3}$. This proves the following description of $U(3)$

Observation A.2.

$$U(3) = \{ \text{diag}(\lambda_1, \lambda_2, \lambda_3) U_{(a,b,c,z)} \text{diag}(1, \lambda_4, \lambda_5) : a, b, c, z, \lambda_j \in \mathbb{T}, j = 1, \dots, 5 \}.$$

By writing $a = e^{i2\alpha}$, $b = e^{i2\beta}$, $c = e^{i2\gamma}$ we get that $U(a, b, c, z) = D'_1 T_{(\alpha, \beta, \gamma, z)} D'_2$, where $D'_1 = \text{diag}(e^{i\alpha}, e^{i(\alpha+\beta)}, -ie^{i(\alpha+\beta)})$, $D'_2 = \text{diag}(1, e^{i\gamma}, -ie^{i\gamma})$ and

$$T_{(\alpha, \beta, \gamma, z)} = \begin{bmatrix} \cos \alpha & -\sin \alpha \sin \gamma & \sin \alpha \cos \gamma \\ -\sin \alpha \sin \beta & z \cos \beta \cos \gamma - \cos \alpha \sin \beta \sin \gamma & z \cos \beta \sin \gamma + \cos \alpha \sin \beta \cos \gamma \\ \sin \alpha \cos \beta & z \sin \beta \cos \gamma + \cos \alpha \cos \beta \sin \gamma & z \sin \beta \sin \gamma - \cos \alpha \cos \beta \cos \gamma \end{bmatrix},$$

providing a parallel description of $U(3)$:

Observation A.3.

$$U(3) = \{\text{diag}(\lambda_1, \lambda_2, \lambda_3) T_{(\alpha, \beta, \gamma, z)} \text{diag}(1, \lambda_4, \lambda_5) : \alpha, \beta, \gamma \in [0, 2\pi], z, \lambda_j \in \mathbb{T}, j = 1, \dots, 5\}.$$

Appendix B

In order to conduct a more detailed study of the alternating projection algorithm we begin by proving the following

Proposition B.1. *Let $A \in U(n)$, $v \in \mathbb{T}^n$ and $P_A(v) = \text{sign}(A^*(\text{sign}(Av)))$. Then, the condition $\|Av\|_1 > n - \delta$ with $0 < \delta \leq \frac{1}{8}$ implies that*

- (a) $\|\mathbf{1} - |Av|\|_2 < \sqrt{2\delta}$,
- (b) $|Av| \geq \frac{1}{2}$ and $|A^*(\text{sign}(Av))| \geq \frac{1}{2}$,
- (c) $\|AP_A v\|_1 = \|Av\|_1$ iff $P_A v = v$,
- (d) $\|P_A v - v\|_\infty \leq 2\sqrt{n}(\|AP_A v\|_1 - \|Av\|_1)^{\frac{1}{2}}$.

Proof.

To see that $|Av|$ is close to $\mathbf{1} = (1, 1, \dots, 1)$ we use $\|v\|_2 = \sqrt{n}$ and observe that

$$\|\mathbf{1} - |Av|\|_2^2 = n - 2\|Av\|_1 + \|Av\|_2^2 = 2(n - \|Av\|_1) < 2\delta,$$

proving (a). This already assures that $|Av| \geq \frac{1}{2}$ for $\delta \leq \frac{1}{8}$ (otherwise $\frac{1}{4} \leq \|\mathbf{1} - |Av|\|_2^2 < 2\delta$, forcing $\delta > \frac{1}{8}$).

Since $|Av| > 0$, we easily see that $\|\text{sign}(Av) - Av\|_2 = \|\mathbf{1} - |Av|\|_2 < \sqrt{2\delta}$. Thus,

$$\|A^*(\text{sign}(Av)) - v\|_2 < \sqrt{2\delta}.$$

Therefore, by the same token as before, $\delta \leq \frac{1}{8}$ implies that $|A^*(\text{sign}(Av))| \geq \frac{1}{2}$.

To prove (c) we note that, by (15) and (16),

$$\|Av\|_1 = \langle v, A^*(\text{sign}(Av)) \rangle \leq \|A^*(\text{sign}(Av))\|_1 \leq \|A(\text{sign}(A^*(\text{sign}(Av))))\|_1 = \|AP_A v\|_1$$

and, therefore,

$$0 \leq \|A^*(\text{sign}(Av))\|_1 - \langle v, A^*(\text{sign}(Av)) \rangle \leq \|AP_A v\|_1 - \|Av\|_1. \quad (22)$$

Thus, $\|AP_A v\|_1 = \|Av\|_1$ implies that $\|A^*(\text{sign}(Av))\|_1 = \langle v, A^*(\text{sign}(Av)) \rangle$, what entails $v = \text{sign}(A^*(\text{sign}(Av))) = P_A v$, since $v \in \mathbb{T}^n$ and $|A^*(\text{sign}(Av))| > 0$.

To show (d) we remark, that $|A^*(\text{sign}(Av))| \geq \frac{1}{2}$ together with $\|A^*(\text{sign}(Av))\|_1 \leq n$ and (22) allows to apply Lemma B.4 below, proving (d). \square

To show Lemma B.4 we start with an elementary observation.

Lemma B.2. *Let $a, b \in \mathbb{C}$ and $0 \leq \epsilon < 1$. If $a + b = 1 - \epsilon$ and $|a| + |b| = 1$ then $\|a\| - \|a\| \leq \sqrt{\epsilon}$.*

Proof. Since $|1 - \epsilon - a| = 1 - |a|$, we get that $(1 - \epsilon)2\operatorname{Re}(a) = (1 - \epsilon)^2 - 1 + 2|a|$, so

$$||a| - a|^2 = 2|a|(|a| - \operatorname{Re}(a)) = \epsilon|a|(2 - \epsilon - 2\operatorname{Re}(a)) = \epsilon|a|\left(1 + \frac{1 - 2|a|}{1 - \epsilon}\right) \leq \epsilon, \quad (23)$$

what is clear for $|a| \geq \frac{1}{2}$, and follows from $\epsilon \leq 2|a|$ in the case when $|a| \leq \frac{1}{2}$. \square

The next lemma can be treated as a solution to a certain random walk problem on the complex plane.

Lemma B.3. *Let $u \in \mathbb{C}^n$. If $\langle u, \mathbf{1} \rangle > 0$, then*

$$||u| - u|_\infty^2 \leq \|u\|_1(\|u\|_1 - \langle u, \mathbf{1} \rangle).$$

Proof. Let $u = (u_1, u_2, \dots, u_n) \in \mathbb{C}^n \setminus \{0\}$. Due to rescaling we can assume that $\|u\|_1 = 1$. Moreover, the problem is insensitive to permuting the entries of u , so it is enough to show that $|u_1| - u_1^2 \leq 1 - \langle u, \mathbf{1} \rangle$. The only hard part is to realize, that this estimate boils down to the previous lemma.

Let us denote $1 - \langle u, \mathbf{1} \rangle$ by ϵ . Since $0 < \langle u, \mathbf{1} \rangle \leq \|u\|_1 = 1$, it is clear that $0 \leq \epsilon < 1$. Moreover, let us set $a := u_1$ and $x := \sum_{k=2}^n u_k$. Clearly, $a + x = 1 - \epsilon$. This means that the circle with the center at a and radius $|x|$ intersects the interval $[0, 1]$ at the point $1 - \epsilon$. Since $|x| \leq \sum_{k=2}^n |u_k| = 1 - |a|$, the circle with the center at a and radius $1 - |a|$ intersects the interval $[0, 1]$ at some point $1 - \epsilon'$ with $0 \leq \epsilon' \leq \epsilon$ (this holds despite the fact, that the intersection can have two points). This proves an existence of $b \in \mathbb{C}$ such that $a + b = 1 - \epsilon'$ and $|a| + |b| = 1$ with $0 \leq \epsilon' < 1$, so Lemma B.2 yields $||a| - a|^2 \leq \epsilon' \leq \epsilon$. \square

Finally, we prove

Lemma B.4. *Let $w \in \mathbb{C}^n$ and $v \in \mathbb{T}^n$. If $0 < \frac{1}{c} \leq |w|$ and $\langle v, w \rangle > 0$, then*

$$\|\operatorname{sign}(w) - v\|_\infty \leq c\sqrt{\|w\|_1(\|w\|_1 - \langle v, w \rangle)}. \quad (24)$$

Proof. Clearly,

$$\frac{1}{c}\|\operatorname{sign}(w) - v\|_\infty \leq \|\bar{w}(\operatorname{sign}(w) - v)\|_\infty = \|v\bar{w} - v\bar{w}\|_\infty.$$

Since for $u := v\bar{w}$ we have $\langle u, \mathbf{1} \rangle = \langle v, w \rangle > 0$ and $\|u\|_1 = \|w\|_1$, the above estimate and Lemma B.3 yield (24) immediately. \square

After proving Proposition B.1 we can take on understanding the workings of the algorithm searching for the biunimodular vectors of a given $A \in U(n)$. Recall that we start with an arbitrary vector $V_0 \in \mathbb{T}^n$ and successively apply P_A (given in Proposition B.1), so that $V_j = P_A^j V_0$, until we reach a J such that

$$\|AV_J\|_1 > n - \delta \geq n - \frac{1}{8} \quad (25)$$

with a certain precision $0 < \delta \leq \frac{1}{8}$. As we mentioned in Subsection 10.1, there is no guarantee that for a given starting vector V_0 we will find $J \in \mathbb{N}$ so that (25) holds. Hence, in practice, the algorithm has to be applied to many random starting vectors in \mathbb{T}^n .

Thus, to facilitate the further discussion of the algorithm, we will concentrate on the starting vectors V_0 satisfying the initial condition

$$\|AV_0\|_1 > n - \frac{1}{8}. \quad (26)$$

Under this assumption we can gather our findings in the following

Proposition B.5. *Let $A \in U(n)$, $V_0 \in \mathbb{T}^n$ and $V_j = P_A^j V_0$ for $j \in \mathbb{N}$. If $\|AV_0\|_1 > n - \frac{1}{8}$, then for all $j \in \mathbb{N} \cup \{0\}$ we have that*

$$(a) \quad \|AV_j\|_1 \leq \|AV_{j+1}\|_1 \leq n,$$

- (b) $V_j \in \mathbb{T}^n$, $|AV_j| \geq \frac{1}{2}$ and $|A^*(\text{sign}(AV_j))| \geq \frac{1}{2}$,
- (c) $\|AV_{j+1}\|_1 = \|AV_j\|_1$ iff $V_{j+1} = V_j$,
- (d) $\|V_{j+1} - V_j\|_\infty \leq 2\sqrt{n}(\|AV_{j+1}\|_1 - \|AV_j\|_1)^{\frac{1}{2}}$,
- (e) $\lim_{j \rightarrow \infty} \|V_{j+1} - V_j\|_\infty = 0$.

Proof. (a) recalls (17) and $\|A\|_{\infty \rightarrow 1} \leq n$. (b) is a matter of a simple induction. If $V_j \in \mathbb{T}^n$ then, by Proposition B.1(b), $|AV_j| \geq \frac{1}{2}$ and $|A^*(\text{sign}(AV_j))| \geq \frac{1}{2}$, so the signum of the latter, that is V_{j+1} , must belong to \mathbb{T}^n . (c) and (d) follow from Proposition B.1. And (e) follows from (d), since (a) assures that the sequence $(\|AV_j\|_1)_{j \in \mathbb{N}}$ is convergent. \square

Since the sequence $(\|AV_j\|_1)_{j \in \mathbb{N}}$ is convergent one can hope, that V_j shall converge to a fix point of P_A . This, however, is hard to assure even under the initial condition (26). This lack of proof for convergence can be traced to the square root appearing in Lemma B.2, that is hard to remove, since (23) gives $||a| - a| \geq \sqrt{\epsilon}|a|$ for $|a| \leq \frac{1}{2}$. Therefore, we can only fall on $\lim_{j \rightarrow \infty} \|V_{j+1} - V_j\|_\infty = 0$ to draw a standard conclusion

Corollary B.6. *If the initial condition (26) holds, then the cluster points of $(V_j)_{j \in \mathbb{N}}$ belong to the set $S_A := \{v \in \mathbb{T}^n : P_A v = v\}$. Moreover, if S_A is finite, then V_j converges to a point in S_A .*

Proof. Here, we use the notation provided in the two previous propositions and by convergence we mean the convergence in any ℓ^p -norm, since they are all equivalent.

Let L denote the limit of $\|AV_j\|_1$. If a subsequence $(V_{j_k})_{k \in \mathbb{N}}$ of $(V_j)_{j \in \mathbb{N}}$ converges to V , then $P_A V_{j_k}$ converges to $P_A V$, since by (b) of Proposition B.5, the sequence $(V_j)_{j \in \mathbb{N}}$ is contained in a closed subset of an open domain, where P_A is continuous. Thus, $\|AV\|_1 = \lim_{k \rightarrow \infty} \|AV_{j_k}\|_1 = L$ and $\|AP_A V\|_1 = \lim_{k \rightarrow \infty} \|AP_A V_{j_k}\|_1 = \lim_{k \rightarrow \infty} \|AV_{j_k+1}\|_1 = L$, so $\|AV\|_1 = \|AP_A V\|_1$. Since $V \in \mathbb{T}^n$ and $\|AV\|_1 > n - \frac{1}{8}$, Proposition B.1(c) implies that $P_A V = V$, hence $V \in S_A$.

If S_A is finite, then its points are separated by open balls. Thus, almost all points of $(V_j)_{j \in \mathbb{N}}$ are contained in the union of these balls. By Proposition B.5(e), there is only one of these balls containing almost all points of $(V_j)_{j \in \mathbb{N}}$, what assures the convergence of V_j . \square

Since $\text{Bi}(A) \subset S_A$, the finiteness of S_A is very hard to establish and, in the Fourier case, brings us back to Conjecture 1.1.

Acknowledgements

Part of this work was carried during several visits of HF to Wrocław, and two visits of ZR to Aachen. We would like to thank our respective hosting organizations. We also thank the referees for providing essential information that made the current understanding of biunimodular vectors more complete.

References

- [1] W. Alltop, *Complex sequences with low periodic correlations*, IEEE Trans. Inform. Theory 26 (1980), no. 3, 350–354.
- [2] J. Backelin, *Square multiples n give infinitely many cyclic n -roots*, Reports Matematiska Institutionen, Stockholms Universitet 1989-No 8.
- [3] J. Backelin, R. Fröberg, *How we proved that there are exactly 924 7-roots*, Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation (ISSAC91), ACM-press (1991).

- [4] H. Bauschke, P. Combettes, D. R. Luke, *Phase retrieval, error reduction algorithm, and Fienup variants: a view from convex optimization*, J. Opt. Soc. Amer. A 19 (2002), no. 7, 1334–1345.
- [5] H. Bauschke, J. Borwein, *On the convergence of von Neumann's alternating projection algorithm for two sets*, Set-Valued Anal. 1 (1993), no. 2, 185–212.
- [6] J. J. Benedetto, R. Benedetto, J. Woodworth, *Optimal Ambiguity Functions and Weil's Exponential Sum Bound*, J. Fourier Anal. Appl. 18 (2012), no. 3, 471–487.
- [7] J. J. Benedetto, I. Konstantinidis, M. Rangaswamy, *Phase-coded waveforms and their design* IEEE Signal Processing Magazine, 26.1 (2009), 22–31.
- [8] I. Bengtsson, W. Bruzda, Å. Ericsson, J.-Å. Larsson, W. Tadej, K. Życzkowski, *Mutually unbiased bases and Hadamard matrices of order six*, J. Math. Phys. 48 (2007), no. 5, 052106, 21 pp.
- [9] P. Biran, M. Entov, L. Polterovich, *Calabi quasimorphisms for the symplectic ball*, Commun. Contemp. Math. 6 (2004), no. 5, 793–802.
- [10] G. Björck, *Functions of modulus 1 on Z_n whose Fourier transforms have constant modulus*, A. Haar memorial conference, Vol. I, II (Budapest, 1985), Colloq. Math. Soc. János Bolyai, vol. 49, North-Holland, Amsterdam, 1987, 193–197.
- [11] G. Björck, *Functions of modulus 1 on Z_n whose Fourier transforms have constant modulus, and “cyclic n -roots”*, Recent advances in Fourier analysis and its applications, Proc. NATO/ASI, Il Ciocco/Italy 1989, NATO ASI Ser., Ser. C 315, (1990), 131–140.
- [12] G. Björck, R. Fröberg, *A faster way to count the solutions of inhomogeneous systems of algebraic equations, with applications to cyclic n -roots* J. Symb. Comput., 12, no.3 (1991), 329–336.
- [13] G. Björck, R. Fröberg, *Methods to divide out certain solutions from systems of algebraic equations, applied to find all cyclic 8 roots*, Analysis, algebra, and computers in mathematical research (Lulea 1992), Lecture Notes in Pure and Appl. Math. 156, 57–70, Dekker, New York 1994.
- [14] G. Björck, B. Saffari, *New classes of finite unimodular sequences with unimodular Fourier transforms. Circulant Hadamard matrices with complex entries*, C. R. Acad. Sci., Paris, Sér. I 320, no.3 (1995), 319–324.
- [15] S. Brierley, S. Weigert, *Constructing mutually unbiased bases in dimension six*, Phys. Rev. A (3) 79 (2009), no. 5, 052316, 13 pp. 81P16
- [16] S. Brierley, S. Weigert, Stefan, I. Bengtsson, *All mutually unbiased bases in dimensions two to five*, Quantum Inf. Comput. 10 (2010), no. 9-10, 803–820.
- [17] R. Cabrera, T. Strohecker, H. Rabitz, *The canonical coset decomposition of unitary matrices through Householder transformations*, J. Math. Phys. 51 (2010), no. 8, 082101, 7 pp.
- [18] E. Candès, Y. Eldar, T. Strohmer, V. Voroninski, *Phase retrieval via matrix completion*, SIAM J. Imaging Sci. 6 (2013), no. 1, 199–225.
- [19] E. Candès, X. Li, M. Soltanolkotabi, *Phase Retrieval via Wirtinger Flow: Theory and Algorithms*, arXiv preprint, arXiv:1407.1065, 2014.
- [20] C.-H. Cho, *Holomorphic discs, spin structures, and Floer cohomology of the Clifford torus*, Int. Math. Res. Not. 2004(35) (2004), 1803–1843.
- [21] P. Combettes, H. Trussell, *Method of successive projections for finding a common point of sets in metric spaces*, J. Optim. Theory Appl. 67 (1990), no. 3, 487–507.
- [22] J. Davenport, *Looking at a set of equations*, Technical Report 87-06, Bath Computer Science, 1987.

- [23] A. De Vos, S. De Baerdemacker, *Scaling a unitary matrix*, Open Syst. Inf. Dyn. 21(4) (2014).
- [24] P. Diță, *Parametrisation of unitary matrices*, J. Phys. A **15** (1982), no. 11, 3465–3473.
- [25] P. Diță, *Factorization of unitary matrices*, J. Phys. A **36** (2003), no. 11, 2781–2789.
- [26] R. Escalante, M. Raydan, *Alternating projection methods*, SIAM, 2011.
- [27] J.-C. Faugère, *Finding all the solutions of cyclic 9 using Gröbner basis techniques*, Computer Mathematics (Matsuyama, 2001), 1-12, Lecture Notes Ser. Comput. 9, World Sci. Publ. (2001).
- [28] J.-C. Faugère, *A new efficient algorithm for computing Gröbner bases without reduction to zero (F5)*, Proceedings of the 2002 international symposium on Symbolic and algebraic computation (ISSAC) (ACM Press), 2002, 75–83.
- [29] F. Fogel, I. WalDSPurger, A. d’Aspremont, *Phase retrieval for imaging problems*, arXiv preprint, arXiv:1304.7735, 2013.
- [30] E. Gabidulin, V. Shorin *New Sequences with Zero Autocorrelation* Problems of Information Transmission **38** no. 4 (2002), 255–267.
- [31] J. Gilbert, Z. Rzesotnik, *The norm of the Fourier transform on finite abelian groups*, Ann. Inst. Fourier **60** no. 4 (2010), 1317–1346.
- [32] R. Gerchberg, W. Saxton, *A practical algorithm for the determination of the phase from image and diffraction plane pictures*, Optik **35** (1972), 237–246.
- [33] M. Grassl, *On SIC-POVMs and MUBs in dimension 6*, Proc. ERATO Conf. on Quant. Inf. Science (EQIS 2004) pp. 60–61, e-print arXiv:quant-ph/0406175
- [34] U. Haagerup, *Orthogonal maximal abelian *-subalgebras of the $n \times n$ matrices and cyclic n -roots*, Doplicher, S. (ed.) et al., Operator algebras and quantum field theory. Accademia Nazionale dei Lincei, Roma, Italy. Cambridge, MA: International Press. (1997), 296–322.
- [35] U. Haagerup, *Cyclic p -roots of prime length p and related complex Hadamard matrices*, arXiv preprint, arXiv:0803.2629.
- [36] M. Idel, M. Wolf, *Sinkhorn normal form for unitary matrices*, Lin. Alg. Appl. **471** (2015), 76–84.
- [37] P. Jaming, *Phase retrieval techniques for radar ambiguity problems*, J. Fourier Anal. Appl. 5 (1999), no. 4, 309–329.
- [38] C. Jarlskog, *A recursive parametrization of unitary matrices*, J. Math. Phys. **46** (2005), no. 10, 103508, 4 pp.
- [39] P. Langevin, G. Leander, *Counting all bent functions in dimension eight* Designs, Codes and Cryptography **59** no. 1-3 (2011), 193–205.
- [40] T.-Y. Li, C.-H. Tsai, *HOM4PS-2.0 para: Parallelization of HOM4PS-2.0 for Solving Polynomial Systems*, preprint.
- [41] F. Mezzadri, *How to generate random matrices from the classical compact groups*, Notices Amer. Math. Soc. **54** (2007), 592–604.
- [42] F. Murnaghan, *On a convenient system of parameters for the unitary group*, Proc. Nat. Acad. Sci. U. S. A. **38** (1952), 127–129.
- [43] K. Nemoto, *Generalized coherent states for $SU(N)$ systems*, J. Phys. A: Math. Gen. **33** (2000), 3493–3506.
- [44] B. Saffari, *Some polynomial extremal problems which emerged in the twentieth century*, Byrnes, James S. (ed.), Twentieth century harmonic analysis—a celebration. Proceedings of the NATO Advanced Study Institute, Il Ciocco, Italy, July 2-15, 2000. Dordrecht: Kluwer Academic Publishers. NATO Sci. Ser. II, Math. Phys. Chem. 33 (2001), 201–223

- [45] M. Reck, A. Zeilinger, H. Bernstein, P. Bertani, *Experimental realization of any discrete unitary operator*, Phys. Rev. Lett. **73** no. 1 (1994), 58–61.
- [46] D. Rowe, B. Sanders, H. de Guise *Representations of the Weyl group and Wigner functions for $SU(3)$* , J. Math. Phys. **40** (1999), no. 7, 3604–3615.
- [47] J. Schwinger, *Unitary operator bases*, Proc. Nat. Acad. Sci. U.S.A. 46 (1960), 570–579.
- [48] C. Spengler, M. Huber, B. Hiesmayr, *A composite parameterization of unitary groups, density matrices and subspaces*, J. Phys. A **43** (2010), no. 38, 385306, 11 pp.
- [49] W. Tadej, K. Życzkowski, *Defect of a unitary matrix*, Lin. Alg. Appl. **429** (2008), 447–481.
- [50] T. Tilma, E. Sudarshan, *Generalized Euler angle parametrization for $SU(N)$* , J. Phys. A **35** (2002), no. 48, 10467–10501.
- [51] T. Tilma, E. Sudarshan, *Generalized Euler angle parametrization for $U(N)$ with applications to $SU(N)$ coset volume measures*, J. Geom. Phys. **52** (2004), 263–283.
- [52] J. von Neumann, *Functional Operators*, volume II, Princeton University Press, Princeton, NJ, (1950). Reprint of mimeographed lecture notes first distributed in 1933.

Hartmut Führ
 Lehrstuhl A für Mathematik
 RWTH Aachen
 52056 Aachen, Germany
 fuehr@matha.rwth-aachen.de

Ziemowit Rzeszutnik
 Mathematical Institute
 University of Wrocław
 50-384 Wrocław, Poland
 zioma@math.uni.wroc.pl